governmentattic.org
"Rummaging in the government's attic"

Description of document:	National Security Agency (NSA) Tales of the Krypt (KRYPTOS Society newsletters) 1994-2003
Requested date:	26-April-2010
Released on Appeal	28-September-2023
Posted date:	01-April-2024
Requested date:	19 March 2024
Released date:	11-July- 2025
Updated date:	25-August-2025
Source of document:	National Security Agency ATTN: FOIA/PA Office 9800 Savage Road, Suite 6932 Ft. George G. Meade, MD 20755-6932 Fax: 443-479-3612 (ATTN: FOIA/PA Office) Submit A FOIA Request Online
Note:	July 1995 KRYPTOS newsletter released 11-July-2025 starts on PDF page 221

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

-- Web site design Copyright 2007 governmentattic.org --

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 61704C
APPEAL: 3959
28 September 2023

This responds to your Freedom of Information Act (FOIA) request of 26 April 2010 for "a copy of each issue of the KRYPTOS Society newsletter (all issues)." A copy of your request is enclosed. Your request has been processed under the FOIA and the documents you requested are enclosed. Certain information, however, has been protected in the enclosures.

Some of the withheld information has been found to be currently and properly classified in accordance with Executive Order 13526. The information meets the criteria for classification as set forth in Subparagraph (c) of Section 1.4 and remains classified TOP SECRET or SECRET or CONFIDENTIAL as provided in Section 1.2 of Executive Order 13526. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave or serious damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in these documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

In addition, personal information regarding individuals has been withheld from the enclosures in accordance with 5 U.S.C. 552 (b)(6). This exemption protects from disclosure information that would constitute a clearly unwarranted invasion of personal privacy. In balancing the public interest for the information you request against the privacy interests involved, we have determined that the privacy interests sufficiently satisfy the requirements for the application of the (b)(6) exemption.

Please be advised that the Agency reasonably foresees that disclosure of the withheld information would be harmful to an interest that is protected by the identified exemptions.

The Central Intelligence Agency (CIA) has asked that we protect information pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)), as well as the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable are Section 6 of the Central Intelligence Agency Act of 1949, 50 U.S.C. 3507 and Section 102A(i)(l) of the National Security Act of 1947, 50 U.S.C § 3024(i)(1). Those withholdings have been marked with the code OGA (Other Government Agency) with CIA identified as the OGA.

The Defense Information Systems Agency (DISA) has requested that personal information regarding an individual be withheld from the enclosures in accordance with 5 U.S.C. 552 (b)(6). Those withholdings have been marked with the code OGA (Other Government Agency) with DISA identified as the OGA.

The Federal Bureau of Investigation (FBI) has requested that personal information regarding an individual be withheld from the enclosures in accordance with 5 U.S.C. 552 (b)(6) and 5 U.S.C. 552 (b)(7)(C). FBI has also requested that information be withheld in accordance with 5 U.S.C. 552(b)(7)(E). Those withholdings have been marked with the code OGA (Other Government Agency) with FBI identified as the OGA.

The National Geospatial-Intelligence Agency (NGA) has requested that information be withheld pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statute applicable is 10 U.S.C. 424. Those withholdings have been marked with the code OGA (Other Government Agency) with NGA identified as the OGA.

The National Reconnaissance Office (NRO) has requested that information be withheld pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statute applicable is 10 U.S.C. 424. Those withholdings have been marked with the code OGA (Other Government Agency) with NRO identified as the OGA.

Since these withholdings may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures.

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

  NSA FOIA/PA Appeal Authority (P132)
  National Security Agency
  9800 Savage Road STE 6932
  Fort George G. Meade, MD 20755-6932

  The facsimile number is 443-479-3612.
  The appropriate email address to submit an appeal is FOIA_PA_Appeals@nsa.gov.

- It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd. - OGIS
College Park, MD 20740
ogis@nara.gov / 877-684-6448 / (Fax) 202-741-5769

Sincerely,

for Sally A.

PAULA A. GILL
Chief, FOIA/PA Division
NSA Initial Denial Authority

Encls:
a/s

TOP SECRET//COMINT

(C) POC: [redacted] info
(U) Last Modified: 11/04/2002 13:04:51
(U)PE EXTERNAL PAGE

(FOUO) The KRYPTOS Society and the Cryptanalysis Career Panel (CACP) are pleased to announce an exciting joint venture - a newsletter, designed to increase communication among the cryptanalysts within the Agency, to provide a calendar of related events, and to provide a forum for the exchange of ideas and questions which impact on the cryptanalytic workforce. This newsletter, which will replace the CACP's CRIB, and the old KRYPTOS newsletter, will be published on or about the first of each month, and will be available on ENLIGHTEN under org.kryptos, and on ESS as topic 1394. Limited numbers of hardcopy editions will be made available to those who are unable to access either of the above.

TABLE OF CONTENTS:

1. Introductory Words
2. Communique from Chief Z
3. Calendar of Events
4. Announcements from the CACP
    a. Professionalizations
    b. Descriptions of new CA Courses
    c. Biography of a new Intern
5. Community Service
    a. MEPP
    b. Z Technical Library
    c. Tech Track News
    d. Cryptolog Update
6. Action Line
7. Technical Topic
8. Telecommunications Training
9. Book Review
10. Puzzle
11. Editorial Corner

(b)(3)-P.L. 86-36

//

1. INTRODUCTORY WORDS

(S) [redacted], the President of the KRYPTOS Council, says: A strong community spirit has always been good for Cryptanalysis. However, with today's technology (e.g., the increased complexity of communications systems, the need to "cryptanalyze" even parts of the system that are not enciphered, the increased pace of change to all parts of these systems), a community that fosters the sharing of information and the ongoing education of its people is becoming absolutely vital to continued success. Couple this technical need with reorganizations, shrinking budgets, new management philosophies, etc. and communication within the CA workforce cries more loudly for attention. With all of this in mind, the Kryptos Society and the CA Career Panel have been looking into ways we can support one another's initiatives, and thus CA in general. One of the more immediate needs was the "simple" dissemination of information. A second need was involving more people in community activities and providing a forum for interaction between junior and senior analysts. This newsletter attends to both needs. We enthusiastically support it and invite your participation and comments.

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

****

(U) [redacted] the Chairman of the CACP, writes: Cryptanalysis has long suffered from a communications problem. Most of us are introverts, and prefer not to give talks or write papers. An unfortunate result of our preoccupation with our own work is a lack of valuable information flowing both from and to the individual analyst.

The KRYPTOS Newsletter will not make any of us into extroverts, but it will allow us to acquire knowledge which could help us do our jobs better. The editors hope to circulate throughout the cryptanalytic community critical current information which many would otherwise have missed.

Some of us, recognizing the importance of interaction among cryptanalysts, will contribute to this effort by writing brief pieces for the Newsletter. All of us can stay abreast of developments in our rapidly expanding career field by reading its pages.

(b)(3)-P.L. 86-36

****
//

2. COMMUNIQUE FROM CHIEF Z

(U) I am pleased to be offered the opportunity to contribute an article to the first edition of the CA newsletter. My first few weeks since replacing Harry Hoover have been rather hectic, with senior promotion boards and the usual influx of spring visitors adding to the usual turmoil of changing jobs and responsibilities. I have now begun arrangements to get out and meet with the people who keep things running in spite of management changes, but that will take some time. In the meantime, let me tell you something about myself, and my views of Z Group and the future.

~~(TS-CCO)~~ I spent my entire career in various parts of the old G Group, until the Spring of 1986 when Harry called me and asked if I would be interested in moving to G03 as [redacted] deputy. During the eight years that followed, I worked with [redacted] and eventually succeeded him as Chief of G03 and then Z03. While this involved me in many parts of Z Group's operations, my time was largely spent in dealing with outside organizations -- [redacted] U. S. industry, in the context of export controls and technology transfer; [redacted] This has given me an interesting perspective on the outside forces that are likely to shape our future effort.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TS-CCO)~~ Future use of cryptographic products is likely to be pervasive, and the technology will be diverse. Much of the plaintext traffic currently used in the Agency's product will be enciphered. Talking to industry, the view is unanimous that there will be a rapidly expanding private sector use of cryptography. Ironically, we see much less enthusiasm on the part of these new potential users, but integration of low-cost or no-cost security features in communications and computer systems is going to make this technology almost universally available to those who choose to use it. The software industry is moving rapidly to incorporate data encryption, data integrity, authentication and access control functions in mass market

(b)(3)-P.L. 86-36

[redacted]

software packages. Cryptographic features are being added to communications hardware systems and computer operating systems. Common carriers are preparing to offer cryptographic products and services. Users will have ready access to an array of security products, and encryption is likely to be applied on top of already enciphered data at different layers in communications networks.

~~(S-CCO)~~ There is considerable pressure from vendors and from privacy advocates for standardization of cryptographic techniques and removal of controls on export of this technology. Moreover, the vendors want standardization based on publicly known algorithms of proven security. However, there is a growing awareness among concerned governments that proliferation of equipment based on such standards would have a significant impact on their national security and law enforcement interests. They are closely following the debate in the U. S. over CLIPPER and CAPSTONE, chips designed by NSA for protection of sensitive but unclassified information They are likely to find similar methods to protect their own sensitive private sector communications. At the same time, most will not rely on commercially available equipment, particularly foreign-manufactured products, to protect their classified systems. The result will be a diversity of indigenous products, ranging in sophistication from manual to state-of-the-art hardware, used for end-to-end encryption independent of any security functions built into the commercial systems used.

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS-CCO)~~ programs and technology controls are important factors in our current and future capability; however, people are without question the one critical factor. Having dealt with these for eight years, I fully appreciate the important role they play in our analytic effort, but they are useless without skilled analysts to develop the techniques that make The Agency has recognized cryptanalysis as its core discipline, and Z Group is blessed with an incredible amount of analytic talent. In my view, our cryptanalysts perform miracles and I'm confident that they will find ways to deal with the formidable problems of the future.

//

(b)(3)-P.L. 86-36

3. CALENDAR EVENTS

June 1	KRYPTOS Talk - Museum (1130-1339) on The Polish Solution of the Enigma - UNCLASSIFIED)
June 1-2	Elder Care Expo (0930-1330, OPS1 N. Cafeteria)
June 1-2	NPIC Expo (0900-1400, 3W156.OPS1) (TK rqrd)
June 2	CMI talk - I. J. Good (0930-1100, Friedman) (Legal Responsibility and Probabilistic

Causation - UNCLASSIFIED)

June 6-10	CRYSCO at CSE
June 8	Z Group Picnic (Burba Lake)
June 13	Z Technology Forum (1300-1400)
June 13-17	CA-305
June 17	CMI Banquet (7 p.m., Holiday Inn, Laurel)
June 20 to Aug 26	SCAMP at La Jolla
June 20 to Aug 12	SCAMP at Princeton
June 21	KRYPTOS TALK - (Friedman, 1300)

UPCOMING

July 7	CMI Talk - (0930-1100, Friedman) [redacted] - New Results in Wavelet Analysis)
July 31	Last day of TSP Open Enrollment
Oct 17-21	[redacted]

(b)(1)
(b)(3)-P.L. 86-36

PLAN AHEAD:

March 27-31, 1995	CARD (GCHQ)
Oct 21, 24-25, 1995	Conference on Computer Communications

//

4. WORD FROM THE CACP -

a. Congrats to those who were recently certified!

[redacted]

(b)(3)-P.L. 86-36

b. The CACP has also provided the descriptions for three new CA course. In future issues we hope to have some reviews from some recent attendees.

CA-104--Introduction to Cryptography and Cryptanalysis (U)

~~(S)~~ Description: This course introduces new cryptanalysts to basic concepts of cryptography and cryptanalysis, including transposition, monoalphabetic substitution through syllabary squares, polyalphabetic substitution, and shift register devices. Basic computer applications are also included.

(U) Duration: Three weeks, full-time.

[redacted]

(U) Student Qualifications: Cleared for Top Secret and Indoctrinated for Special Intelligence.

****

CA-112--[redacted] (U)

(b)(3)-P.L. 86-36

(S) Description: This course will teach the student a variety of cryptanalytic applications using programs from packages such as

[redacted]

(U) Duration: Three weeks, full-time.

(U) Student Qualifications: Successful completion of CA-110 and CA-123. Students must be cleared for Top Secret and indoctrinated for Special Intelligence. Assigned to NSA/CSS.

(b)(1)
(b)(3)-P.L. 86-36

****

CA-219--Advanced Cryptanalytic Techniques (S)

Description: This course enables the cryptanalyst to evaluate various [redacted] techniques to select the best one to use in a given situation. The course is highly interactive and some problems require teamwork to solve. Computers are used throughout the course. Primary topics

[redacted]

Duration: Two-three weeks, full-time.

Student Qualifications: Successful completion of CA-261 and CA-223 or equivalent experience with the material contained in the courses.

****
****

c. (S) BIOGRAPHICAL PORTRAIT (Each month we will introduce one or two of the most recent people to have joined either the CA Intern program or the CA Tech Program. In the future we may also include interviews with some of the more senior members of the CA community.)

[redacted] the first new intern in fiscal year '94, is presently assigned to Z4333. In her second tour, she is working on several projects, including [redacted]

[redacted]

****

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36
(b)(6)

[redacted]

[redacted] came on board in June of 1993 and entered the intern program in July. "The variety of mathematical applications, diversity of the work that is done in cryptanalysis, and simply the 'challenge' of being able to break a cryptanalytic system," she says, "is what interested me in this field."

[redacted] (b)(6)

//

5. COMMUNITY SERVICE

a. Mathematics Education Partnership Program (MEPP)

Back to School

by [redacted]

The desks seem small, the occupants short. I feel confused and gigantic as my dazed eyes scan the Lilliputian scene before me. There is so much noise! Laughter and shouts bounce off the walls and a hundred (or maybe only 32) young, wriggling bodies try to find comfort for hyperactive limbs in the confines of sharply angled desks.

"Okay, students, settle down now," says the teacher.

My initial reaction to this is immediate. I look in vain for an empty seat to leap into, hastening to obey the teacher's instruction. Then I remember: I don't have to sit down. I'm not a kid anymore. Oh, yeah.

"Class, we have a speaker today from NSA who's going to talk to us about codes and ciphers. Will you all please give her your attention?"

I take a deep breath and smile. I remind myself that there's really nothing to be scared of. I'm the adult here. Besides, these kids have to listen to me because I'm bigger than them. Wow! A captive audience. I think I'm going to like this.

This school year, NSA's Mathematics Education Partnership Program handled approximately 1600 requests from area schools for speakers from NSA to give presentations on a wide variety of math-related topics. Of the 1600 requests, the MEPP was able to fulfill over 1200. While the objective of the Math Speakers Bureau is to increase student interest in mathematics, the benefits of the program extend beyond this to include the speakers themselves.

I volunteered for the Math Speakers Bureau because I thought it might be fun to convey some of my interest and enthusiasm for cryptanalysis to students. Okay, I thought, a few times a month I'll go and say my

(b)(3)-P.L. 86-36

[redacted]

piece to some school and that will be that. A small contribution to the community and a chance to get out of the office every once in a while. No big deal. Well, I was wrong.

For one, I discovered how much I enjoyed teaching. I loved being able to talk about something that I think is really neat and try to find a way to get others to think so, too. The experience of revealing the mysteries of monoalphabetic substitution ciphers to students, who, for the most part, were practically falling all over themselves with excitement, was a new one. I couldn't remember the last time anyone had ever listened so hard to what I was saying. The excitement was contagious.

I also found that I really enjoyed working with students in the 12-13 age group. They were old enough to demonstrate sharp mental skills but still young enough to be unafraid to show their enthusiasm. (This was not quite the case with two high school classes I spoke to whose participants seemed more eager to be excused to go to the bathroom or to pass unenciphered notes to each other!) I was impressed by the skills and behavior shown by 6th and 7th grade students and there were more than a few whom I would have given serious consideration to adopting!

And I was given the chance to revisit my own days in school--to once again see walls adorned with brightly colored posters on everything from subject and verb agreement to world geography to recess rules. To smell that peculiar perfume of chalk dust and slightly spoiled milk which only schools seem to have and to however briefly feel the connection between my school days and my present. To be surrounded by youth in all its manifestations, both large and small. It was like taking an elixir for the illness of routine and tunnel-visioned maturity.

As you can see, I can't say enough good things about being a speaker for the MEPP. It has been a truly enriching experience for me and, I hope, for the students I have spoken to. For more information, contact [redacted] MEPP coordinator, at [redacted] See you in 7th grade!

****

b. Z TECHNICAL LIBRARY

(U) Although the use of the Technical Library has increased substantially since the formation of Z Group, we would like to remind everyone of this valuable resource and encourage you to take advantage of it.

[redacted]

(b)(3)-P.L. 86-36

(U) You can browse through library holdings and then request a library paper without leaving your desk. Simply call the "tlc" system administrator, [redacted] on [redacted] and she will set

[redacted]

up an account on "bimini" which will allow you to search for, and request, documents via "tlc". We have prepared a handbook to help you use "tlc", and you can get a copy from the library.

(C) You can also stop by the library or call [redacted] with a request. [redacted] will reproduce the document requested - originals never leave the library. Normally, you will receive the document within a working day of your request. Obviously, compartmented papers are subject to greater restriction. Eventually, we will have softcopy versions of papers so that we can satisfy a request electronically.

(C) To keep you current on new additions to the library, a newsgroup, [redacted] has been added to ENLIGHTEN. It is updated monthly. For those without ENLIGHTEN, a printed version is available.

(U) We hope this information will encourage you to use the Z Technical Library. If your organization has any technical documents which can be donated to the library, please call [redacted] Suggestions on how the library can improve its services are also welcome.

****

c. TECH TRACK CORNER

The DDO Honey Pot
by [redacted]

(b) (3) -P.L. 86-36

With regard to the Tech Track:

DDO has a large fund available for technical health needs, but no one seems to be aware of it. This money can be used for textbooks, conference expenses, or any technical health purpose not covered adequately by conventional funding. Requests should be made through the Group Plan Director for the Tech Track, in our case Floyd Weakley for Z. However, requests can be presented to anyone associated with the tech track, e.g. TTRP members or skill field reps, career panels, etc., who can in turn make a formal request through Floyd. The plus side to the bureaucracy associated with the Tech Track is that there are lots of people around who are involved, and should be able to help.

****

d. CRYPTOLOG

(FOUO) CRYPTOLOG has a new editorial staff which is working to revitalize the publication. With a focus on the informal exchange of information and ideas among SIGINT professionals, articles are being sought which promote exchange and understanding among our technical disciplines. In that spirit, you are invited to contribute articles, letters and reviews to CRYPTOLOG. [redacted] is the Cryptanalysis representative on the Board of Advisors. She can provide editorial guidance and will be happy to accept articles for publication.

****

//////////

6. ACTION LINE

[redacted]

(U) QUESTION: The comment was made at the 1994 CA Conference that, whereas morale had been a problem the previous year, it no longer was now. I think what really happened is that there was such a clear non-response to morale problems that people quit discussing it.

(U) Management in Z Group has yet to respond to some of the morale problems created by the reorganization, and should provide some means of communicating these problems to management, other than town meetings that can put those with complaints in a high pressure, potentially embarrassing situation.

signed "sleepless in Z"

ANSWER: From Chief Z

~~(S-CCO)~~ The 1993 CA Conference was held less than a year after the DDO restructuring, the creation of Z Group, and a major internal reallocation of resources. Not surprisingly, the changes that were taking place created some unease within the workforce and were the cause of some of the morale problems surfaced by the Conference participants. In particular, the drawdown of the effort against the Soviet problem and the reallocation of resources to other problems left a number of people uncertain about their future. Many were moved to new jobs, some requiring new skills. Some of the organizational changes resulted in confusion over roles and responsibilities. In retrospect, there are clearly things that could have been done to handle this transition more smoothly.

(U) While there was less attention focused on morale during the 1994 Conference, I certainly don't interpret this to mean that we have solved all of the problems that were cited in the 1993 Conference report. I hope that we can make more progress toward this objective in the coming year. Input such as that provided by the Conference attendees is invaluable in identifying the kinds of problems that we should be focusing attention on, and I hope that we can find other means to allow individuals to comfortably communicate such concerns. We have an exceptionally talented workforce in Z Group and a challenging set of problems facing us in the future. We cannot afford to let poor morale or lack of motivation prevent full and effective use of our talent.

****

~~(C)~~ QUESTION:
a) How many people are C/A certified?
b) What is the breakdown by grade?
c) Currently, how many aspirants are there?

signed, "an aspiring cryptanalyst"

(b)(3)-P.L. 86-36

ANSWER: Provided by [redacted], CACP Exec

a. As of 24 May 1994, there are [redacted] professionalized Cryptanalysts here.
b. The breakdown by grade is:

SLE [redacted]

[redacted]

SCE
15
14
13
12
11

c. There are [redacted] aspirants; the distribution by grade follows:

GRADE	ASPIRANTS
15	
14	
13	
12	
11	
9	
7	
5	
4	
Military	
Enlisted	
Officer	

(b)(3)-P.L. 86-36

An aspirant for Cryptanalysis certification is anyone who has registered with the Cryptanalysis Career Panel, [redacted], with the intention of pursuing professionalization in Cryptanalysis. Registration consists of submitting a recent Personnel Summary, which includes job experience descriptions and lists of training courses completed. Professionalization in Cryptanalysis requires the successful completion of six major categories:

1. Three years cryptanalytic experience
2. Three diversity assignments, each at least six months in length
3. Training courses, as described in the criteria document CA-104, CA-107, CA-110, CA-112, CA-123, CA-219, CA-223, CA-261, CA-D01, EG-243, MP-119, and either MP-220 or MP-227
4. Passing the CAPQE
5. Approved Technical Paper
6. Approved Computer Program

****

(U) QUESTION: Is it true that the Z Group Vision Statement was recently changed? If so, why and by whom or by what committee? Also, how does the new statement differ from the old one?

Signed by "curious in Z"

ANSWER: Provided by Tom Yodzis, the Z TQM Coordinator

"Yes, the Z Vision Statement was changed, though not recently. About a year ago, Mr. Hoover felt that the original Vision Statement could be more effective if it were shortened.

Thus, "Turning Today's Challenges Into Tomorrow's Successes Through Innovative Cryptanalysis" became "To Read Tomorrow's Enciphered

Communications". This new vision is presently being put on plaques for mounting at several highly visual points within Z Group. They should be seen shortly."

****

(FOUO) QUESTION: "Why does the CA Intern Program, whose graduates go mostly to Z group, reside in Personnel, while the CMP program, whose graduates mostly leave Z group, warrant its own division in Z?"

ANSWER: Provided by [redacted]

The Cryptologic Mathematician Program (CMP) was established to support the entire mathematics community at NSA, not just Z Group. Each technical Key Component invests billets in the program and reaps a return on its investment in the form of graduates, roughly in proportion to the number of billets invested. Of the approximately [redacted] CMP graduates still at NSA, about [redacted] are in the Operations Directorate. Most of that [redacted] are in Z. In recent years, the rate of CMP billet support from Z has increased to about [redacted]--and the proportion of graduates staying in Z has risen to about [redacted] over the past five years. (b)(3)-P.L. 86-36

For the rest of the question, let's review a little history. There had been a major math hiring effort in 1951-2, known as the Junior Mathematician Program, but that was not sustained. The Cryptologic Mathematician Program was established in 1963, when it became clear that there was going to be a sustained and rather large math hiring effort again. Since most of the new hires were assigned to the Operations Directorate, the Operations and Personnel managers at the time agreed that it should be administered in Operations, and P1 was given the responsibility to run the program.

Just a few years later, other disciplines decided that they, too, would benefit from a program similar to the CMP. This time, though, the Personnel managers decided to set up a career development program, to include career panels; and such a comprehensive effort, they decided, should be run from the Administrative Key Component. The first intern program to be established was for cryptanalysis, and several others were set up in quick succession. Although many of these programs were geared to Operations, not all were, which gave additional support to the notion that the intern programs should be run from Personnel.

When the Mathematics Career Panel was established, they decided not to set up a mathematics intern program, because the CMP was already in existence and meeting that need. I think there have been questions raised from time to time about why the CMP is in the OD, and the best answer may be that it was just a matter of timing. The CMP was first, and it was successful; and there has never been much motivation to dislodge it from Operations. It became a division because the reorganization of the OD in 1992 did away with its former home base, P1.

You may be interested in knowing that there is at least one other officially recognized Agency program which enjoys a status similar to that of the CMP--the Resident Signal Engineering (RSE) Program, administered in R5. It was established several years ago, well after the advent of the intern programs, and was modeled after the CMP.

[redacted]

[redacted] (b)(3)-P.L. 86-36

7. TECHNICAL EXCHANGE -

[redacted] from Chris Copple, [redacted]

(Editor's note: Chris' Technical exchange artical was classified at a level that was not allowed on this home page. We have removed it so that the remaining articles could be viewed. Those within Z group can see the entire newletter including Chris' article

here

8. TELECOMMUNICATIONS TRAINING

(C) The Z Telecommunications Training Board (ZTTB) was established by Chief Z to help ensure that the Z work force is adequately trained in modern telecommunications technologies. These technologies are having and will continue to have a significant impact on Z Group targets and missions. Collection, processing, and [redacted] all are essential to our mission and all are affected by technological advances.

(C) Last year, the Z Telecommunications Training Working Group (ZTTWG), a group of Z technical experts, studied needed and available training. They surveyed available training courses, both NCS and external, and evaluated them on their applicability to Z Group needs. The ZTTWG report recommended creation of a standing group to address training issues, and the ZTTB is that group.

(C) The ZTTB works to identify necessary training needs and find suitable presentations. It is investigating overview training as well as tightly focused offerings. In addition to reviewing and recommending established classes in NCS and from external sources, the board sponsors the development of in-house seminars which take advantage of the many subject matter experts in Z Group. One example of this approach was the recent one-day seminar on data compression, presented on May 17. The board is also working to acquire videotapes of selected talks, to be available from the Z Library.

(C) It is imperative that we in Z know what telecommunications systems are doing for us and to us. The bit fairy cannot be trusted these days (never could be, really). [redacted]

(b)(1)
(b)(3)-P.L. 86-36

[redacted] (b)(3)-P.L. 86-36

[redacted] Z needs analysts who are able to exploit modern telecommunications fully.

(b)(1)
(b)(3)-P.L. 86-36

(U) If you are a supervisor, you should encourage your people to take advantage of the training opportunities. Also, you should develop a list of necessary knowledge and skills, and make these needs known to the ZTTB through your office representative.

(U) Individuals should look for ways to expand their knowledge. If you find something good, let others know. It doesn't have to be a class or a seminar-a good book is gold. Find out what you need to do your job and make your supervisor aware of your needs.

(U) The board is interested in high quality presentations, and so seeks out and listens to feedback on training events. If you attend a valuable session, let your office representative know, so we can make more people aware of it. If a training event is not all that it should be, we want to know that, too.

The members of the ZTTB are:

[redacted]

//

9. BOOK REVIEW: APPLIED CRYPTOGRAPHY [redacted] Reviewer)

(b)(3)-P.L. 86-36

Applied Cryptography, for those who don't read the internet news, is a book written by Bruce Schneier last year. According to the jacket, Schneier is a data security expert with a master's degree in computer science. According to his followers, he is a hero who has finally brought together the loose threads of cryptography for the general public to understand. Schneier has gathered academic research, internet gossip, and everything he could find on cryptography into one 600-page jumble.

The book is destined for commercial success because it is the only volume in which everything linked to cryptography is mentioned. It has sections on such diverse topics as number theory, zero knowledge proofs, complexity, protocols, DES, patent law, and the Computer Professionals for Social Responsibility. Cryptography is a hot topic just now, and Schneier stands alone in having written a book on it which can be browsed: it is not too dry.

Schneier gives prominence to applications with large sections on protocols and source code. Code is given for IDEA, FEAL, triple-DES, and other algorithms. At first glance, the book has the look of an encyclopedia of cryptography. Unlike an encyclopedia, however, it can't be trusted for accuracy.

[redacted]

Playing loose with the facts is a serious problem with Schneier. For example in discussing a small-exponent attack on RSA, he says "an attack by Michael Wiener will recover e when e is up to one quarter the size of n." Actually, Wiener's attack recovers the secret exponent d when e has less than one quarter as many bits as n, which is a quite different statement. Or: "The quadratic sieve is the fastest known algorithm for factoring numbers less than 150 digits..... The number field sieve is the fastest known factoring algorithm, although the quadratric sieve is still faster for smaller numbers (the break even point is between 110 and 135 digits)." Throughout the book, Schneier leaves the impression of sloppiness, of a quick and dirty exposition. The reader is subjected to the grunge of equations, only to be confused or misled. The large number of errors compounds the problem. A recent version of the errata (Schneier publishes updates on the internet) is fifteen pages and growing, including errors in diagrams, errors in the code, and errors in the bibliography.

Many readers won't notice that the details are askew. The importance of the book is that it is the first stab at putting the whole subject in one spot. Schneier aimed to provide a "comprehensive reference work for modern cryptography." Comprehensive it is. A trusted reference it is not.

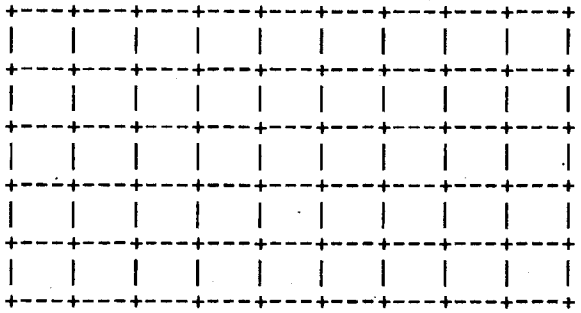
****
//////////

10. PUZZLE

9 to 5

Nine of the clues below lead to 5-letter words which are to be entered vertically into the diagram. The other clue gives a word of 9 letters which can be entered horizontally in the middle row. The clues are in no particular order; it's up to you to figure out which words go where. As a help, all of the letters for the 5-letter words are taken from the 9-letter word. Solution next issue.

bury	tips
evildoer	worth
unmoving	up
because	misdeed
Le Havre Holy	sting



Send your answers to [redacted], and next month we will publish the names of those who correctly solved this puzzle.

****

(b)(3)-P.L. 86-36

[redacted]

//

11. EDITORIAL CORNER

If you have a relatively short technical treatise which you think might appeal to our readers, please submit it to any of the editorial board.

In fact, if you have anything you would like to have considered for inclusion in future issues, please forward it, IN ASCII format, to one of the POCs listed below.

We would very much like this newsletter to represent a broad cross-section of the CA community - we need some more volunteers to help us, however. Perhaps you would like to work on one of the topics in this issue, or perhaps there is another topic which you think should be included in future issues. Either way, we would like your input, and help, so give one of us a call. The more people who divide up the work, the less burden on any one person.

NOTE: We MUST receive any submissions for the July issue by 24 JUNE.

****

EDITORIAL BOARD

[redacted]

[redacted] Puzzle Editor [redacted]

Jack Ingram, Cryptologic History Museum

[redacted] NCS

OFFICE Reps

[redacted]

[redacted] (b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

(b)(3)-P.L. 86-36

[redacted]

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

(b)(3)-P.L. 86-36

TOP SECRET//COMINT

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:16
(U)PE EXTERNAL PAGE

CA NEWSLETTER
ISSUE 2
JUNE 1994

//

NOTICE NOTICE NOTICE NOTICE NOTICE NOTICE NOTICE NOTICE

This will be the last issue of the newsletter mass-mailed to all of Z. All future issues will be posted to ENLIGHTEN (under org.kryptos) and also available through ESS (1395). For those who are unable to access either ENLGIGHTEN or ESS, we will set up an e-mail alias. Please let your Office POC know if you need this service.

//

TABLE OF CONTENTS:

(b)(3)-P.L. 86-36

1. Perspectives in CA
2. Calendar of Events
3. Announcements from the CACP
   a. Professionalizations
   b. Intern Biography
   c. CA Survey Recap
4. Technical Health
   a. Tech Track Corner
   b. Z4 and Technical Health
   c. Technical Exchange
5. Community Service
   a. Adopt-a-School
6. Action Line
7. Book Review
8. Puzzle
9. Name the Newsletter Contest - WIN AN ICE CREAM SUNDAE!!
10. Editorial Corner

//
---

1. PERSPECTIVES IN CA - (We will be asking CA Seniors to contribute their insights. We hope to feature both a Z and a non-Z perspective each month.)

a. ~~(S-CCO)~~ [redacted] Chief [redacted]

NSA's research is a series of links, each with a distinct but overlapping role to play in assuring that current and future cryptanalytic challenges are met successfully. For cryptanalysis these links form a circular chain which extends from an outside organization, IDA/CCR, to teams of analysts in various Z Offices. Each link plays an important role, [redacted]

(b)(3)-P.L. 86-36

utility of this link is evident to all and it works very well. [redacted] is

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

9/23/2010

Z's window to the outside world. It administers grants programs, provides our interface with IDA/CCR, provides theoretical research on general questions of cryptanalytic interest and finally and most importantly it contributes directly to Z problems in terms of integrees, directly working on Z problems, and participation in SCAMPs, miniscamps, expert conferences, working groups, and seminars such as ACE and CARD.

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

In today's environment of swift technological change, a viable technical organization such as Z must guard against the propensity to use all of its energy fighting today's problem, otherwise it will surely lose tomorrow's battle. Research is not a luxury, it is a necessity.

[Editor's note: Joe has also started to write a short historical perspective on this subject which may be published in a future newsletter.]

****

(b)(3)-P.L. 86-36

b. (U) [redacted] Chief R51 - AN R51 FABLE

(Editor's note: [redacted] R51 Fable was classified at a level that was not allowed on this home page. We have removed it so that the remaining articles could be viewed.)

In order to see the entire newsletter click here

//////////

2. CALENDAR OF EVENTS

UPCOMING

July 1-4	First Annual Meadefest (Burba Lake - 1730 on the 1st, 1200-2300 July 2-4)
July 4	Fireworks at Burba Lake

[redacted]

July 7	CMI Talk - (0930-1100, Friedman) ([redacted] - New Results in Wavelet Analysis)
July 8	KRYPTOS Literature Contest Papers Due (POC [redacted])
July 11	Z Technical Forum "Modem Error Correction" by [redacted] (1300-1400, OPS 2B, Rm #6) (see TECHNICAL EXCHANGE for more details)
July 31	Last day of Thrift Savings Plan Open Enrollment
Aug 8	Z Technical Forum Talk - Asynchronous Transfer Mode (ATM), by [redacted]
Aug 15 - Sep 15	Flexible Employment Open Season
Aug 20	Aviation Appreciation Day - Tipton Airfield
Aug 21	Raindate for Aviation Appreciation Day
Oct 17-21	[redacted]

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

PLAN AHEAD:

March 27-31, 1995	CARD (GCHQ)
Oct 21, 24-25, 1995	Conference on Computer Communications

//

3. WORD FROM THE CACP -

a. (U) Congratulations to our most recently certified cryptanalyst - [redacted]

****

b. ~~(S)~~ INTERN BIOGRAPHY (Each month we will introduce one or two of the most recent people to have joined either the CA Intern program or the CA Tech Program. In the future we may also include interviews with some of the more senior members of the CA community.) Two CA interns are responsible for these profiles. [redacted] interviewed this month's Intern, and [redacted] drafted the article.

(b)(3)-P.L. 86-36

****

~~(SC)~~ [redacted] is currently working on her first tour in Z431. She is assigned to [redacted]

[redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) [redacted] saw the intern program as a chance to finally get over to "the other side of the house" and try cryptanalysis firsthand. In fact, it was her interest in cryptanalysis that brought her to the Agency. Meeting an NSA recruiter at a career fair her senior year of

[redacted]

college led her to research the history of cryptanalysis. She decided that the Agency's mission sounded much more interesting and worthwhile than most of the other jobs available.

(b) (6)

[redacted]

c. (U) [redacted] Chairman of the CACP, has brought to our attention a briefing recently presented to the CACP by three Z412 cryptanalysts who conducted a survey relating to CA certification. (A recap of their findings is presented below.) Bob would like to add that the CA Panel would be interested in other ideas too.

(b) (3)-P.L. 86-36

Dear Cryptanalysts:

You might think that we are the founders of the Cryptanalysis Liberation Front, but au contraire! Actually, we are just three concerned cryptanalysts.

After listening to several frustrated co-workers in Z4 who are trying to get professionalized in CA, we decided to approach upper management with our concerns. We were encouraged to research the possible problem areas and to present our findings to the CA Panel.

With the help and guidance of [redacted] the career development advisor in Z4, we formulated a course of action. Wanting to know how other cryptanalysts in Z Group felt about this topic, we created a survey. We asked the Chairman of the CA Panel, another member of the CA Panel and the chief of Z41 to review the questions on the survey to obtain their comments and suggestions before it was sent out. The survey was e-mailed to division level management requesting that it be passed to all members in their division. We received over 130 responses. We also called seven other career panels in order to accumulate their professionalization criteria and statistics. In addition, we talked to M33 to get information about the Job Task Analysis (JTA) procedure and status. A JTA is performed to obtain legally defendable professionalization criteria for a career field. Finally, we acquired a copy of the Work Transition Force's report on the needs of NSA's work force in the year 2000.

Using the above mentioned data, we gave presentations to the Z4 Technical Advisory Board (Z4TAB) and the CA Panel at their June meetings. Based on survey comments, we proposed some alternatives to the current professionalization criteria and procedure. The members of the CA Panel were very interested in the thinking of the cryptanalytic community and expressed their desire for aspirants to seek their counsel.

One of the slides in our presentation that you might find particularly interesting contained the results of the survey for those that are certified. (Sections of it are presented below.)

***** Certified *****

Number of people surveyed: 90

4. Number of attempts to pass?

Exam: 1-5 Paper: 1-4 Program: 1-3

6. What part caused difficulties?

[redacted]

Exam: 32 Paper: 12 Program: 9

8. Satisfied with the CA professionalization?

Yes: 37 Neutral: 11 No: 31

9. A written exam of the type currently used is a good measure of cryptanalytic ability?

Yes: 64* Neutral: 8 No: 14 (*many of these said "Yes, but...)

10. Having writing and oral skills is a good idea for professionalization?

Yes: 77 Neutral: 6 No: 4

11. Having programming skills is a good idea for professionalization?

Yes: 69 Neutral: 5 No: 14

12. Would you like a CA professionalization where a person can choose to be professionalized in one of a number of specialty areas that best describes her or his career field?

Really bad idea:	19
Bad idea:	24
Neutral:	14
Good idea:	19
Really good idea:	13

We would like to thank not only those who responded to the survey but also those who showed great interest and support during the entire project.

We have a handout of the slides we used in the briefing, a handout containing all the comments from a random sample of a third of the respondees, the letter from the Chairman of the CA Panel in response to our briefing and a copy of the survey in softcopy form. If you have not yet received any of these via e-mail and you would like them, they are available. If you are in Z, please ask your Division Chief, as they were sent to Zdistro3. If you are not in Z, e-mail any of us with your request.

Sincerely,

[redacted]

(b)(3)-P.L. 86-36

****

//

4. TECHNICAL HEALTH

a. (FOUO) TECH TRACK CORNER

The Cryptanalysis Technical Track, submitted by [redacted]

I. Current Technical Track Review Panel (TTRP)

Voting Members: [redacted] Chairman,

[redacted]

[redacted]

[redacted] Floyd Weakley [redacted] joined as new members in June

Non-Voting: [redacted] Z Plan Executive
[redacted] CA Panel Asst. Executive

II. Current CA Title Distribution: (includes TTRP members)

(b)(3)-P.L. 86-36

Member	Senior Member	Master
[redacted]		

Note: There is no "expected" or pre-set distribution. These numbers represent those who were the first to apply, including those selected to serve on the Panel itself, evaluated against the published criteria for CA Titling.

III. Needed: A few more good cryptanalysts!

New tech track applications continue to come in. Those from the more senior members of the community are especially encouraged, since

(1) The use of titles allows quick identification of the resources available in the community, when special needs arise;

(2) Promotion boards are being advised to consider technical track status, and

(3) Technical titles may soon be used in the selection process for newly established titled technical positions.

The process is relatively simple: Submit the one page application form, accompanied by a current persum, to the CA Panel Office. Any of the listed panel TTRP members can be contacted for information or advice on the application process.

****

Below is the current title distribution for Z personnel who have applied to some of the other TTRPs. (These statistics DO include the members of the various TTRPs.) This information provided by [redacted] Exec for Z Tech Track Plan.

	Member	Sr. Member	Master
Math	[redacted]		
Computer Systems			
Signals Analysis			
Intelligence Analysis			
Signals Collection			
Engineering			

****

b. (U) Z4 and Technical Health

(FOUO) There is a new Z4 newsgroup on ENLIGHTEN called "z4.technews". It is going to be used by the Z4 TAB (Technical Advisory Board) to post information related to technical issues in Z4. This board was formed

[redacted]

by Chief, Z4, for the purpose of advising Z4 management about the technical health of Z4. The current membership is [redacted] (b)(3)-P.L. 86-36

[redacted]

(U) Z4 technical health items which will be posted are announcements for seminars, courses, technical talks, diversity tours, the Z mentor/resource program, reference documents, and contact points for new technology. Since this is a Z4 newsgroup, it could also be used to exchange information on operational problems, cryptanalysis, tools, techniques, etc. If you are posting an article containing target information, please do not cross post (post in groups outside Z).

(U) We understand that not all Z4 is using/trained in ENLIGHTEN. Until that happens, we will be operating in a parallel mode and sending this information out via e-mail.

(U) If you have any suggestions for Z4 TAB actions, please post your comments/questions in z4.technews or e-mail any TAB member. We look forward to hearing from you and starting an active exchange of information.

****
The following information was posted in z4.technews

~~(C-SCO)~~ The Z4 TAB has created the following list of technologies along with points of contact who are willing to answer any question regarding the topics. If you have additions to this list, please post/e-mail. An additional list of mathematical techniques and cryptologics and associated points of contact will be posted/e-mailed later.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

NEW COMMUNICATIONS TECHNOLOGY

[redacted]

(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

PROCESSING and DATAFLOW

[redacted]

c. TECHNICAL EXCHANGE -

(1). Z Technical Forum Presentation - (July 8th - see CALENDAR for details)

[redacted]

(U) The classification of the talk is TSC.

****

(2). PROBLEM OF THE WEEK - (from [redacted] cryptanalyst)

(b)(3)-P.L. 86-36

[redacted]

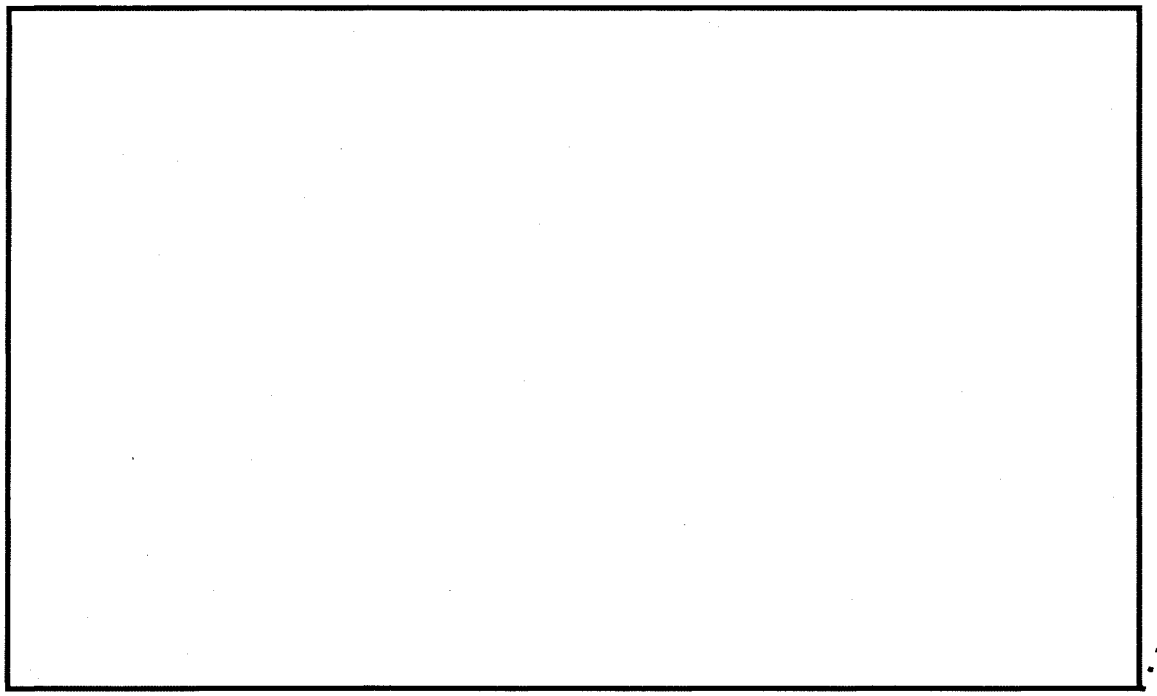
(U) I would like to make sure everyone is aware of the Problem of The Week offering that is currently available. The Problem of The Week group began when a few cryptanalysts in Z441 started to work the "London Times" Sunday crossword puzzle at lunch. (If you have never tried it you might enjoy it. The puzzles have "cryptic" clues--their terminology not mine. A single puzzle may take several lunches to finish.) As we began to solve the puzzles more quickly, we started looking for something else to do at lunch. Several members were studying for the MAY 1994 CAPQE, so I received permission from the CA Panel to distribute problems from the NOV 1993 CAPQE. I began to e-mail one problem per week to each interested person in Z441. Each person would work the problem individually, but invariably discussion would break out on how things were proceeding and who had the "neatest" solution. We found that almost every problem had an easy solution, a hard solution, and a very hard solution (e.g. exhaustion). I decided to expand the effort to include all of Z44 in my e-mail alias. Well, it did not take long for the list to include people from all of Z4 and then all of Z.

(U) Here is how the Problem of the Week works. One problem from the last CAPQE is sent out each Monday morning as an attachment to an e-mail message. A solution, including a narrative of the technique used, is sent each Friday morning. The problems are meant to be fun exercises which can be used to keep your skills sharp and help you learn new techniques. Each problem is designed to be solved in half an hour or less. I had hoped that people would try the problem by the middle of the week and if necessary seek help within their office before receiving the answer on Friday. I heard that some people were not having the open discussion like we have in Z441, so we started meeting on Friday mornings in 1S037 at 11:00 to toss around the problem of the week. Activity waned as the May 1994 CAPQE approached.

(U) New problems will soon begin arriving in the mail, including the spanking new May 1994 problems. If you are interested in receiving the problems and solutions in the mail and are not already receiving them, please contact me at [redacted] Also, if you are trying a problem and get stuck, please e-mail or call me at [redacted] and I will give you a hint.

(b)(3)-P.L. 86-36

***



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

****

//////////

5. COMMUNITY SERVICE

(U) a. ADOPT-A-SCHOOL PROGRAM

NSA-Meade High School's Adopt-A-School program has completed its first school year. A joint effort initiated by the Deputy Director for Support Services and the National Cryptologic School, the program has had approximately 190 volunteers who have contributed close to 1500 hours.

Volunteers have participated in various activities such as tutoring, mentoring, guest speakers, helping to repair school equipment, and computer installation and maintenance. The school has received file cabinets, blackboards, old books from the library, and furniture. Despite the tremendous support the program has received from the NSA work force, help is still needed. Below is a list of activities and coordinators for the Adopt-A-School program printed with the permission of the NSA program coordinator for publicity. Feel free to contact the POC's directly if you are interested in volunteering. DDS has granted admin leave for this volunteer program.

(b)(3)-P.L. 86-36

SUMMER WORKSHOPS

1. Citizenship Tutorial
Three week workshop preparing students for the state mandated exam.
12 - 28 July, 1200 - 1400
Tuesday and Thursday
POC:

2. Writing Workshop
"How to Write Research Papers"
12 - 28 July, 0800 - 1000
Tuesday and Thursday
POC:

3. Mentoring Seminars
The first seminar in July will focus on helping to develop self-esteem. Other mentoring seminars will follow. Note: These seminars are for existing mentors. Similar seminars will be developed for those wishing to become mentors. For more information contact

NSA SUPPORT TO MEADE HIGH SCHOOL
DIRECTORY OF ACTIVITIES

STUDENT SUPPORT

Tutoring Programs

1. Math and Science Help
   After-Hours Clinic
   POC: [redacted]

2. Language Help
   After-Hours Clinic
   (Spanish, German, French)
   POC: [redacted]

3. Reading Assistance
   In-class remedial reading program
   POC: [redacted]

4. Writing Assistance (new)
   Writing Lab
   POC: [redacted]

5. Social Studies Assistance (new)
   POC: [redacted]

Mentoring Programs

1. Educational Talent Search
   Mentoring program for the
   1st time college students
   POC: [redacted]

2. Female Role Models
   After-hours mentoring program
   POC: [redacted]

3. Black Male Role Models
   After-hours mentoring program
   POC: [redacted]

Hobby Clubs

1. Chess
   POC: [redacted]

2. Genealogy (new)
   POC: [redacted]

3. Gaming
   POC: [redacted]

4. AT&T Investment Challenge
   POC: [redacted]

FACULTY SUPPORT

1. Computer Software Support
   Ad-hoc training teachers in
   DB3, LOTUS, WORD PERFECT
   POC: [redacted] or [redacted]

2. Database Support
   Admin support to Maryland
   Tomorrow Program
   POC: [redacted]

3. In-Service Staff Training
   E2 presentation on Learning Styles
   POC: [redacted]

4. Athletic Department Support
   Assist coaching/
   coordinate with Agency
   POC: [redacted]

FACILITIES & EQUIPMENT

1. Computer Hardware
   Donations and Ad-hoc support installing computers
   POC: [redacted]

2. Excess Equipment Transfer

3. Facilities Repair, Furniture and Material Donations
   Donation of excess furniture, books, maps, posters, etc. Consultant

[redacted]

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

for installing folding doors, repairs to sound system, utility vehicle, popcorn maker, and future---building walls, installing fence, and telephone lines
POC: [redacted]

(b)(3)-P.L. 86-36

Administrative leave has been authorized for those who participate in the program (PML 1-94, 28 Jan 94). If you would like to volunteer or need further information the POCs are listed below.

Program POCs

[redacted] (Program Manager), [redacted]
[redacted] (NSA program coordinator, publicity), [redacted]
[redacted] (OGC), [redacted]
[redacted] Public Relations Advisor), [redacted]

//

6. ACTION LINE

(U) QUESTION: I have recently heard a rumor that promotion boards have been instructed to consider a person's tech track title during promotion reviews. Is this true? If so, isn't the tech track in danger of becoming what everyone predicted - another hoop to jump through? Please set the record straight on this matter.

Signed -

Still Willing To Be Convinced

****

ANSWER: (We asked a number of people to respond, and they did. Responses follow in the order received.)

(U) a. From [redacted] Ex-Chair of the Z GG14 Promotion Board:

(b)(3)-P.L. 86-36

Although my term as president of the Z 14 Board has expired (new board not named yet), I will nonetheless venture a response to the question you have submitted.

I am quite certain that most promotion boards and their members suffer from an overabundance of "guidance", official and otherwise. There are many areas of professional and personal achievement which a promotion board must consider in evaluating all eligible candidates. Education, certification(s), sex, race, performance and potential, and training are some of these areas; there are others. The trick is how to accommodate all the guidance, be faithful to your own sense of right and fairness, and then, after much agonizing select a few good ones from the many good ones. The fact that one holds a Tech Track Title is a professional accomplishment and needs to be considered, but this is a subjective, not a mandated, consideration.

****

(U) b. From [redacted] Chair of the Agency GG15 Promotion Board:

During the period the FY94 board was sitting there were no notations in the promotion records regarding Tech Track Status. So the short answer is, "no, we were not instructed to consider tech track status". Board members did glean from the persums and from the nomination records whether individuals were in technical, technical management or management positions, and we kept ourselves aware throughout the selection process of the relative share of promotions

going to each of those categories.

When the Technical Track is incorporated into the formal record, promotion board members will surely take membership into consideration. The boards are always faced with a dilemma: there are more people deserving promotion than there are promotions to award; so, every legal factor available will be used to select the MOST deserving from the group. If all other factors appear equal in a competition between two individuals and one holds an advanced technical track title, the promotion will go to the title holder. Or, put in another way -- If you were a technical track master and saw someone in your field get promoted who had not bothered to participate in technical track at all, what criteria would you think a selection board was using?

Technical Track title requirements strike me as far more than "hoop jumping". The requirements describe performance and behavior standards that clearly define the characteristics of a professional who is committed to the continuing development of the art and science of the field. It is not a meaningless exercise to identify and recognize such people, particularly when this recognition process is managed by peers in the field. It is these people who are the high potential performers, the strength of this agency and the guardians of our future. And, interestingly enough, those are also the people we want to promote!

~~SECRET~~//FOUO

(U) c. From [redacted] Chair of the Agency GG14 Promotion Board:

Promotion Boards are seeing less and less discrete data. With the new performance appraisal system, boards are down to the promotion write-up, the persum, and awards. When doing a zero-based review at the Agency level of some [redacted] GS-13's, any merit-based indicator is bound to take on added significance.

(b)(3)-P.L. 86-36

If my memory serves me right, the records we reviewed did show that a person was 'tech track', but with no titles. Titles -- or descriptions that more or less matched them -- have begun to show up in promotion write-ups.

It is certainly true that technical qualifications in general, and tech track participation in particular, carry increasing weight in the GG-14 promotion process. Recent GG-14 promotion statistics will bear this out. We received no specific guidance to "consider a person's tech track title." We were, however, charged to increase the number of technical promotions--and that's how it should be.

(U) d. From [redacted] Chair of the DDO GG14 Promotion Board

The new DDO-14 board is not yet making explicit use of Tech Track Status. In fact, that information is not recorded in the data we have been given so far. We will first see that (albeit an incomplete version) information when we get write-ups and will then make some use of that information. Lack of a title, will not prevent an individual's promotion; having a title (and which title) will be a positive statement about that particular individual's technical accomplishments. In other words, we will use it in a way analogous to the way we use information about awards that the candidate has received; this is in contrast to professional certification which is a "hoop". Hope that answers your question.

Please encourage people to pursue titles. In general, the tech track criteria are specific, mission-oriented and reasonably objective.

[redacted]

Boards will come to rely more and more on that information as they are denied the other information that boards have traditionally used.

****

(U) e. From George Cotter, Chair of the Senior Tech Track Board (STTB)

Agency promotion boards have not received guidance as yet on tech track titles. The new system is still being installed, there is not yet sufficient parity among the ten fields in respect to membership to permit firm guidance in my view.

However, I certainly would like to comment on the implication that tech track titles are meaningless - "another hoop to jump through" is the expression used in your submission. If the STTB has done its job right, and the Agency's TTRP's are objectively applying criteria and standards, titles represent the status of an individual in a core cryptologic profession, judged by peers. We have used hundreds of very good technical people to try to get this right and if we have, titles are hardly meaningless.

To go one step further, though, tech track membership will carry with it the responsibility for participants, and their management, to enhance an individual's technical competencies under a variety of initiatives. We advance the overall technical health of the Agency principally by developing our technical work force into better cryptanalysts, mathematicians, etc. Most people would conclude that this should add to the significance of titles. And advancement in the program should therefore merit higher ranking in promotion boards, shouldn't it?

Yes, I believe, in time, promotion boards at all levels will take tech track titles into consideration in evaluating promotion candidates, since titles should reflect the judgment of the leaders in the field of the competency of the tech tracker. If I were serving on a promotion board, I would certainly value that input.

****

(U) f. From [redacted] Chair of the Z 13 Promotion Board

My board was not given specific guidance about rewarding tech track members, but we WERE given guidance to promote the very few we can afford to, based on performance and potential. This obviously includes technical accomplishments in an organization like Z Group. We do consider tech track titles to be an indication of technical competence and professional resolve and commitment, along with other information such as awards and letters of appreciation, etc. There is not yet a place in official records to show technical title, although we see them in persums and promotion writeups. So it is important for each eligible candidate to include such information in his/her persum. Our board has a tech track representative on it, as do most boards.

(b)(3)-P.L. 86-36

****
//////////

****
//////////

7. LITERARY TIDBITS

(U) Hidden Messages in Tolkien Fiction - (by [redacted]

[redacted]

If you've ever thumbed through a copy of J.R.R. Tolkien's trilogy The Lord of the Rings, you might have been inclined to glance quickly at the title page. If so, you might have noticed the strange and decorative borders at the top and bottom of the page. But did you know that the letters there, written both in runes and in a more elegant freehand, actually spell out intelligible text?

Fortunately, the key to these hidden messages is readily available. It is found at the end of Book Three, The Return of the King, in the extensive appendices. This key may be applied not only to the "Ring" trilogy, but also to The Silmarillion, Unfinished Tales, and perhaps other books. Here are the translations of the hidden messages. You'll have to figure out what the proper names mean.

The Lord of the Rings -- The Lord of the Rings, translated from the Red Book of Westmarch by John Ronald Reuel Tolkien: herein is set forth the history of the War of the Rings and the return of the King by the hobbits.

The Silmarillion -- The tale of the First Age, when Morgoth dwelt in Middle Earth and the Elves made war upon him for the recovery of the Silmarils. To which are appended the Downfall of Numenor and the history of the Rings of Power and the Third Age in which these tales come to their end.

Unfinished Tales -- In this book of unfinished tales by John Ronald Reuel Tolkien, brought together by Christopher Reuel Tolkien, his son, are told many things of Men and Elves in Numenor and in Middle Earth from the Elder Days in Beleriand to the War of the Rings, and an account is given of the Druedain, the Istari, and the Palantiri.

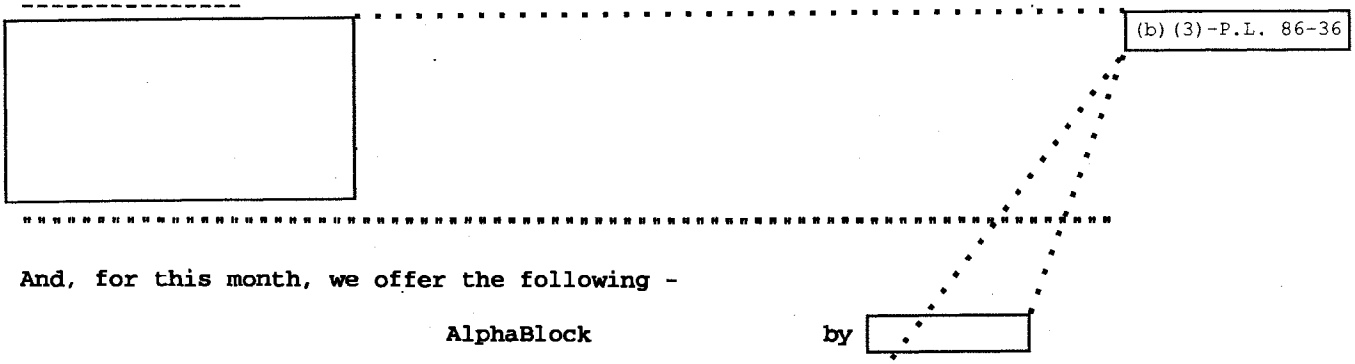
****
//////////

8. PUZZLE

And now, the solution to last month's puzzle

```
-----------------
A C R S M I S S I
C R I A E N M I N
M I S C R E A N T
E M E R I R R C E
S E N E T T T E R
```

JUNE'S SOLVERS:



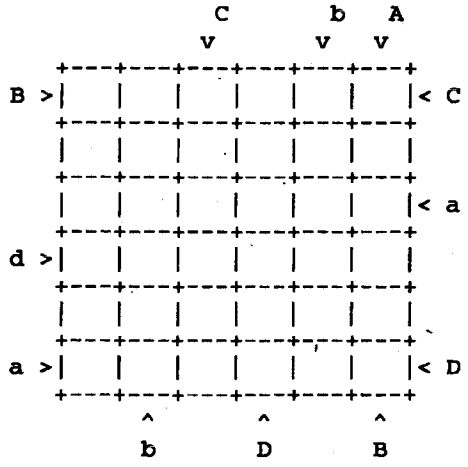
****

And, for this month, we offer the following -

AlphaBlock by

Each row and each column in the diagram below contains one each of the letters A, B, C and D, as well as two blank spaces (though not necessarily in that order). The letters around the diagram are clues

to the location of the letters within the diagram: a capital letter indicates the first letter encountered in that row or column when traveling in the direction of the arrow; a lower-case letter indicates the second letter encountered in that row or column when traveling in the direction of the arrow. From the clues given, can you determine the placement of all of the letters?



//

9. CONTEST

A number of people have entered the "Name This Newsletter Contest" - must be the lure of the coveted double scoop sundae being offered to the winner which prompted such efforts. Now we'd like your help. Select your three favorites, list them in priority order, and send them, by COB 8 July, to any member of the editorial board. We will tabulate the results, and the August edition will carry the new banner. Here are the suggested names:

TRANSCRYPT
TransCrypt
Playfair Square
Plain & Cipher
The Graph Paper
Colored Pencils
The Log Waits
The Racing Form
The Approximator
Monthly Plain Text
The Odds' Log
Cryptographic Crier
The SECRET Finder
THE CRIB
The Kryptogram
Tales of the Crypt
The Cryptanalytic Highway
The CA Digest
CA Today
CA Review
CA News
CA World
Plain Text on Cryptanalysis
Plain Text

(b)(3)-P.L. 86-36

[redacted]

CA Cornucopia
CA Scene
The NewsBreaker
The CipherSpace
URCA
BIT-BY-BIT

****
//////////

10. EDITORIAL CORNER

If you have a relatively short technical treatise which you think might appeal to our readers, please submit it to any of the editorial board.

In fact, if you have anything you would like to have considered for inclusion in future issues, please forward it, IN ASCII FORMAT, to one of the POCs listed below. Also, PLEASE paragraph classify each item submitted.

A reminder that anonymity may be requested for Action Line items - in fact, you may mail them in hardcopy form to a POC is you wish.

We would very much like this newsletter to represent a broad cross-section of the CA community - we need some more volunteers to help us, however. Perhaps you would like to work on one of the topics in this issue; perhaps there is another topic which you think should be included in future issues. Perhaps you would be interested in joining the Editorial Board. Anyway, we would like your input, and help, so give one of us a call. The more people who divide up the work, the less burden on any one person.

NOTE: We MUST receive any submissions for the August issue by 22 JULY.

****

EDITORIAL BOARD

[redacted]

[redacted] Puzzle Editor, [redacted]

[redacted] Problem of the Month Editor, [redacted]

Jack Ingram, Cryptologic History Museum

[redacted] NCS

OFFICE Reps

[redacted]

(b)(3)-P.L. 86-36

[redacted]

~~~~~~

PSSSSST! SNEAK PREVIEW OF NEXT MONTH'S ISSUE!

an article on the KRYPTOS Society
a profile on a KRYPTOS Distinguished Member
an ACTION LINE item on selection CACP members and Chairman
an article on the VOYNICH Manuscript
a challenging acrostic puzzle
the winner of the NAME THE NEWSLETTER CONTEST

and many many more !

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

(b)(3)-P.L. 86-36
~~~~~~

TOP SECRET//COMINT

~~(C)~~ POC: [redacted] info
(U) *Last Modified: 11/04/2002 13:04:51*
(U)PE EXTERNAL PAGE

****
* TALES FROM THE CRYPT *
****

ISSUE 3

August 1994

//

TABLE OF CONTENTS:

1. Perspectives in CA
   a. [redacted]
   b. [redacted]
2. KRYPTOS Society
3. Calendar of Events
4. News from the CACP
   a. Announcement of new chairman
   b. Recent Professionalizations
   c. Announcement of new Panel Member
   d. New Intern and new C/A Tech
   e. Biography of a New CA Technician
   f. CACP Response to Z4 Survey
   g. New Gold Bug Team Award
   h. CA112 - Report on the Pilot Course
5. Technical Health
   a. Z2 Summer Program
   b. SPICE
   c. Conscrypt
   d. Science & Engineering Society Presentation
   e. Solution to July Problem of the Month
   f. August Problem of the Month
6. Technical Article - Just the Fax
7. Norman Roberts Award - Call for Nominees
8. Action Line
9. Literary Tidbits
10. Puzzle
11. Contest
   a. Last month's winner
   b. New contest
11. Editorial Corner

//
---

1. PERSPECTIVES IN CA - (We will be asking CA Seniors to contribute their insights. We hope to feature both a Z and a non-Z perspective each month.)

****

~~(FOUO)~~ a. [redacted] Special Assistant to Z3

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

Z PERSPECTIVE ON CA

(U) Some of the most disgruntled people I have known at NSA were experts at what they did, did it well, and did it for many years. But then the Agency's need for their particular specialty diminished, and they became increasingly frustrated as recognition and promotions eluded them. Eventually, they were moved to new offices where they were the neophytes and everyone else seemed like experts. The frequent result was a "retirement in place".

(U) How do we avoid this scenario? There are several good answers which come to mind. The first is that one may be so totally aware of the big picture that they can see that sometime in the future system X or country Y or technology Z will no longer be important to the United States, so they take steps not to be stuck in those areas. Not all of us have this kind of prescience, but if you do, more power to you.

(TSCUO) A second answer is to keep your technical skills current. If you took your math and CA courses in the early 80's and only have a steady listing of CA305 on your Persum since, you may be out of date. Today the disciplines of math, CA, communications theory, and computers all intertwine as they advance by leaps and bounds. If you keep up, you will have a wide choice of rewarding jobs where you can contribute. At present, there is a wealth of courses, seminars, workshops, and talks available. You may even study something on your own, or with a group of co-workers. I recently read a budget-conscious statement that too many people were taking courses for which they had no operational necessity, and that this would have to stop. I hope that attitude does not prevail.

(U) The third answer is to diversify. I happen to sit on Z Group's math TTRP (hold the applause, please), and diversity is definitely one of the important criteria we consider. For some people, the biggest move of their careers has been from G421 to Z21, or from G41 to Z4. Of course, diversity is possible even within these organizations, but that is frequently not what is happening. Why not work in signals for a while, do some diagnosis, try speech or hand systems, do reverse engineering, seek a PCS tour, program computers, go to Z03, or get involved in developing SPD's? The contacts you establish and the new friends you make will enrich your career as much as the new knowledge you gain. One brilliant Hungarian mathematician switched every five years to a totally different branch of mathematics. We don't all have his genius, but few of our jobs require genius, just hard work and a willingness to learn.

(U) You may ignore all this advice, be lucky, and have a wonderful career. I sometimes think this is what has happened to me. I'm not a big-picture guy, and my course work definitely leaves something to be desired. But I have at least known instinctively when it was time to change jobs, seek a new challenge, or learn some new discipline which I needed. I hope you can be more deliberate than I.. Take charge of your own careers and don't wait for "them" to do it for you. If things go sour, it's poor satisfaction if all you can do is blame "them" for it.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(TSC) b. [redacted] SUSLO-2 , [redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted] - U.S. CRYPTANALYSTS IN THE U.K.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted] is a small division of cryptanalysts and mathematicians working at Government Communications Headquarters (GCHQ), Cheltenham, England, U.K. for the Special U.S. Liaison Officer, London (SUSLOL),

[redacted]

The U.S. has had a close SIGINT with the U.K. for the last 50 years. We are now assisting each other in making strategic decisions for the post cold war era.

//

[redacted]

(b)(3)-P.L. 86-36

(U) 2. KRYPTOS SOCIETY

What is the KRYPTOS Society, and Why Should You Join?
The KRYPTOS Society, an NSA professional organization of cryptanalysts, was established in 1981 to promote interest in cryptanalysis, to provide a focal point for fields of common interest to cryptanalysts of the National Security Agency, and to promote excellence in professional cryptanalytic activity throughout the cryptologic community.

The Society promotes professionalism in cryptanalysis by:

- Sponsoring talks of general interest at its quarterly meetings as well as at other times during the year. Topics are related to CA on both historical and current projects

  (On June 1, KRYPTOS sponsored a luncheon, at the National Cryptologic Museum, which included a presentation by [redacted] on the Polish solution of the ENIGMA. Following this, individuals viewed the museum exhibits at their own pace, vastly aided by a cadre of knowledgeable guides. On June 21st [redacted] briefed on a much more current topic, [redacted])

- Sponsoring an annual literature contest and awarding cash prizes and plaques at the annual luncheon.

  (Prizes for first, second, and third places are $250, $150, and $100, respectively.)

- Recognizing sustained excellence in the cryptanalytic field through selection of Distinguished Members of the KRYPTOS Society. The Distinguished Members are inducted at the annual luncheon. To date, [redacted] people have been inducted as Distinguished Members of the KRYPTOS Society.

- Holding an annual luncheon in the fall. At this event, a highlight of the KRYPTOS year, members of the Society and their guests gather at a local restaurant to enjoy lunch, socializing, and to collectively recognize professional achievement.

**** - Co-sponsoring the annual fall CMI-KRYPTOS picnic.

- Coordinating, with the CACP, the publication of this newsletter.

Join us! We need your membership and your input to give voice to the cryptanalysts in our community now and in the future. This is an excellent chance for networking at all levels. To join, just fill out the attached application, and send it, and $5.00 to -

[redacted]

**** - HELP/INPUT NEEDED! Would you prefer a Spring Picnic? A Dance? Something else? We would like to do something which appeals to the community - please let anyone on the KRYPTOS Council know if you have any suggestions.

~~~~~~

**** KRYPTOS MEMBERSHIP APPLICATION DUES: $5.00 (Annually)****

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]
~~~~~~

MEMBERSHIP YEAR: 1994 ( ) NEW ( ) RENEWAL

NAME:_____ DATE: _____

SECURE PHONE: _____ NON-SECURE: _____

ORG: _____ BLDG: _____

INTERESTED IN CHAIRING A COMMITTEE? ____YES ____NO

INTERESTED IN WORKING ON A COMMITTEE? ____YES ____NO

CHECK COMMITTEES OF INTEREST TO YOU:

____ CRYPTANALYTIC LITERATURE ____ MEMBERSHIP

____ DISTINGUISHED MEMBERS ____ PUBLICITY ____AWARDS

____ PROGRAMS ____ NEWSLETTER ____ RETIRED MEMBERS

~~~~~~
v
//

3. CALENDAR OF EVENTS

UPCOMING

Aug 1-5	SPICE ([redacted] on MAGMA)
Aug 9	Science & Engineering Society - "Advanced Technologies for Signal & Data Processing" (1300 - R&E Symposium Center (More info in Section 5d)
Aug 11	CLA Presentation - "Being a Second Party Linguist" (1300, 9A135)
Aug 15	GOLD BUG TEAM AWARD Ceremony
Aug 15 - Sep 15	Flexible Employment Open Season
Aug 20	Aviation Appreciation Day - Tipton Airfield
Aug 21	Raindate for Aviation Appreciation Day
Sep 8	CMI - "Modern Results on an Ancient Problem" (0930, Friedman)
Sep 12	Z Technical Forum Talk - Asynchronous Transfer Mode (ATM), by [redacted]
Sept 19-21	Cryptanalytic Computing Conference (SRC)
Sep 20	Security Day (Friedman, 1000 & 1300)

(b)(6)

(b)(3)-P.L. 86-36

[redacted]
~~~~~~

(b)(1)
(b)(3)-P.L. 86-36

Oct 17-21 [redacted]

Oct 19-21 ESCAPE `94 (Biennial ciphony experts' conference) - NSA

Oct 27 KRYPTOS luncheon

Oct 31-Nov 4 CONSCRYPT at CSE

PLAN AHEAD:

March 27-31, 1995 CARD (GCHQ)

//

4. WORD FROM THE CACP -

a. (U) LATE-BREAKING NEWS - AS WE GO TO PRESS!!!! The CACP has just announced that the new Chairman-elect is [redacted] Deputy Chief of Z4. [redacted] will take over officially on the 1st of November.

b. (U) Congratulations to our most recently certified cryptanalyst, [redacted]

c. (U) The CACP is pleased to announce that [redacted] has just joined the Panel.

d. (U) There are two other new faces in the CA community. Our newest Intern is [redacted] and the newest member of the CA Tech Program is [redacted] A warm welcome to both!

(b)(3)-P.L. 86-36

****

e. (U) BIOGRAPHICAL PORTRAIT (Each month we will introduce one or two of the most recent people to have joined either the CA Intern program or the CA Tech Program. In the future we may also include interviews with some of the more senior members of the CA community.)

****

[redacted]

(SC) [redacted] is in his first tour in Z433 as a CA technician. [redacted]

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) [redacted] became interested in the program after speaking with [redacted] the Assistant Exec to the CACP, and looks forward to the diversity of the CA programs.

[redacted]

(b)(3)-P.L. 86-36
(b)(6)

[redacted]

(b) (3)-P.L. 86-36
(b) (6)

****

f. ~~(FOUO)~~ CACP RESPONSE TO Z4 SURVEY

The Cryptanalysis Career Panel has met to consider possible changes to its certification criteria which have been suggested by the well-researched and well-presented (by [redacted] at the Panel's June meeting; [redacted] also contributed greatly) "Cryptanalysis: 2000 or Bust" survey.

In that survey it was made abundantly clear that a sizable number of contributing cryptanalysts, in particular those performing duties in some, but not all, of the Z4 offices, are disadvantaged by the conjunction of the Panel's current criteria and the demands of their current assignments. Especially, challenges were issued concerning our required paper, program, and examination.

We agree that the duties with which some cryptanalysts are regularly engaged may make it less convenient for them than for others to satisfy the demands of writing a suitable paper. The issue of a program is less clear, for nearly all modern cryptanalytic personnel routinely face situations in which a correct computer program could contribute significantly to the solution of a problem.

Cryptanalysts need to share their ideas so that we all may benefit. Failure to announce successful cryptanalytic methods can lead to solvable problems remaining unexploited or being solved only after a deplorable duplication of effort. The Panel, responsible for the health of the profession, feels strongly the need to continue the requirement of the written and verbal enrichment of our rapidly growing discipline in this way. Aspirants know that acceptable cryptanalytic papers need not be based on one's own work, but must show an understanding of good cryptanalytic technique. If one's own area does not lend itself well to such an endeavor, a six-month diversity tour may well provide an opportunity.

Cryptanalysis as a discipline is in a period of rapid transition. Nowhere is that change as evident as in the ubiquitous use by successful cryptanalysts of modern computing machinery. This is a trend which will not be reversed, and today's cryptanalyst simply must possess programming skills. Our required program need not be (and almost never is) a 3000-line optimized virtuoso performance. Many successful cryppies have only rudimentary programming skills, but they must be able to compose rapidly an effective routine in a high-level language when the need arises. Familiarity with existing routines is a very useful asset, but the professional cryptanalyst should be expected to bring more weapons into the battle.

Agency budget cutbacks will lead to reductions in all skill fields, and Cryptanalysis will necessarily be hurt. We must each learn to do more. A cryptanalyst with skill in only one area risks redundancy, as many of us have recently learned. The PQE is designed to measure cryptanalytic ability across our discipline, and we administer the examination in part to encourage the development of individual flexibility which Cryptanalysis needs to flourish. A movement in the opposite direction, toward specialization, would stifle the growth we are trying to cultivate.

(b) (3)-P.L. 86-36

[redacted]

In summary, the Panel feels that at this time, when increased proficiency is being demanded of every cryptanalyst, no action should be taken to lower the standards of excellence by which professional cryptanalysts are judged. We also feel that provisions to accommodate specialists within the community would be counterproductive.

In spite of the Panel's seemingly intransigent position, we are as anxious as are the aspirants in our community to close the gap between their attainments and our requirements. We propose to do that by suggesting methods of achieving our published objectives.

Let us first consider the examination, since we regard it as the most demanding requirement for certification. We acknowledge that the examination does a poor job of simulating the work environment of any cryptanalyst. We would love to be able to, in a way which is equitable to all aspirants, prepare our examination so that computer tools can be brought to bear. We are not close to realizing our goal. We cannot counter the argument that many of our cryptanalytic successes are at least partly dependent upon cleverly contrived computational coups. Few cryptanalysts attack any significant problem today without computer support.

But a still more important component of cryptanalytic success, one which we all value beyond computer facility, is the ability to design attacks to solve challenging cryptanalytic problems. It is this problem-solving capability which our examination is designed to measure. We conjecture that if cryptanalysts were asked to identify the trait which good cryptanalysts share in greatest abundance, a plurality would respond "Problem solving."

Cryptanalysts who fare poorly on the PQE should consider broadening themselves through diversity tours, coursework, and study sessions. We notice that a recent effort by [redacted] to make problems (and solutions) from old examinations available to aspirants has met with little enthusiasm in Z4. We feel so strongly that problem-solving skills are essential to cryptanalytic success that we are led to question the suitability for cryptanalytic careers of those who refuse to avail themselves of such an opportunity.

There may be some misunderstanding of the requirements for authorship of successful papers. We emphasize, and we have mentioned this before, that the cryptologic accomplishment recorded need not be original. A service is provided by someone who well records, and explains the significance of, any cryptologic triumph, and we seek to recognize that contribution. The requirements for completion of this task are currently being rewritten (as are the requirements for an acceptable program) and should be available for dissemination soon.

Individual initiative is a necessary ingredient in the certification process. Our Panel Executives are always available to discuss requirements, and can often suggest avenues available to determined aspirants. Few take advantage of this service, and we cannot hold the aspirant for certification blameless if he/she fails to take this painless and potentially rewarding step.

We are aware that opportunities to complete our requirements vary with the office in which the cryptanalyst is employed, but individual cryptanalysts should not stay rooted in a single office for long periods of time. We regard mobility as very important in our field, and we feel that most managers agree with this view. Of course

(b)(3)-P.L. 86-36

an analyst who chooses not to acquire diversity may suffer from lack of opportunity, but we feel that the responsibility to negate this handicap rests with the individual.

In this response to the very important issues raised by the "Cryptanalysis: 2000 or Bust" survey, we hope we have made clear our strongly held opinion of the direction in which Cryptanalysis is moving. We see ahead a rapid expansion of our field, reacting to enormous transitions in telecommunications technology. We must, individually and collectively, respond to this challenge by continuing to expect maximum performance from each cryptanalyst. We are willing to entertain the possibility of altering the criteria, but not of weakening them.

We understand that this policy does not meet the needs of those cryptanalysts who have chosen to specialize in one particular aspect of our art. We have respect for specialists; we benefit from their achievements. But for our community we view any specialization as unhealthy, leading to a segregation and parochialism which, with cryptanalysts in such short supply, we can ill afford. We urge specialists to become more versatile, to exercise their abilities in other areas, to promote the free flow of cryptanalytic excellence. Cryptanalysis is expanding, not contracting, and we will all need to broaden our horizons to meet the challenges ahead. Professional cryptanalysts will respond to our entreaties.

****

g. The GOLD BUG and GOLD BUG TEAM AWARDS -

The Gold Bug Award was established in 1982 to recognize outstanding technical excellence and achievement in the field of cryptanalysis. [redacted] then Chairman of the Cryptanalysis Career Panel, was instrumental in establishing this NSA/CSS Exceptional Cryptanalytic Achievement Award and giving its name. The award consists of a pin suitable for wearing on a lapel or dress, a certificate signed by the Director, and a plate bearing the recipient's name attached on a permanent plaque that is installed in the hallway of the first floor OPS #2B.

In his introductory remarks at the dedication of the GOLD BUG Award plaque, Cryptanalysis Career Panel Chairman [redacted] announced, "Edgar Allen Poe, the author of the story 'The Gold Bug' which give its name to the award, was an amateur cryptanalyst. He had hoped to gain employment with the federal government as a cryptanalyst, and achieved, in his failure, the fame that has been denied our honorees in their successes. Poe once said, 'It may well be doubted whether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve.' The recipients of the Gold Bug Award have demonstrated human ingenuity at its zenith."

(b)(3)-P.L. 86-36

Criteria for selection are:

a. the achievement to be rewarded must be of professional calibre as defined by the goals and objectives established by the Cryptanalysis Career Panel;

b. the achievement must be in cryptanalysis; and

c. the nominee must be actively engaged in cryptanalysis within the Cryptologic Community.

[redacted]

There are currently [ ] recipients of the GOLD BUG Award, the last awarded to [ ] in March 1994.

In early 1994, the Cryptanalysis Career Panel received nominations for outstanding cryptanalytic achievement performed by teams of cryptanalysts. The excellence of the technical work was noteworthy, but the original GOLD BUG Award was established to recognize individuals. So the Cryptanalysis Career Panel approved the creation of a similar award for team achievement. The concept was approved by the Director, and the first recipients were selected.

[ ] [ ] all of Z211, will be honored in a ceremony on 15 August. The DDO will unveil the new plaque at that ceremony. A plate bearing the names of the recipients will be attached to the new permanent plaque to be installed in the hallway of the first floor OPS #2B. The GOLD BUG TEAM Award plaque will hang next to the GOLD BUG Award plaque.

(b)(3)-P.L. 86-36

****

h. CA-112 Pilot Course

(U) Our first issue previewed some new CA courses. Here is a follow-up, provided by [ ].

(FOUO) A pilot offering of CA-112 was held in May. Although there were numerous problems with computers and computer hookups that need to be ironed out, overall the pilot went very well. We hope to resolve most of these problems by setting up a separate computer network in E4 designated solely for CA classes. Each section of the course was introduced by a short lecture given by a cryptanalyst considered an expert on that topic. Toys were developed from real problems worked throughout Z-group. Most toys were worked on [ ] with a few being done directly on the SUN workstations. The course covered a variety of DPP and [ ] programs as well as [ ] [ ].

(FOUO) The students were very bright, hard-working individuals who took very seriously the responsibility of critiquing the modules and suggesting changes for the future. The major recommendation was to ensure that the course focused on using CA applications and techniques to learn UNIX programs. Most other recommendations dealt with rearranging portions of the class or changing the emphasis of various toys. Revisions are currently under way for the four classes of CA-112 scheduled for FY95.

(FOUO) Student comments included such things as: the course was enjoyable and valuable, even in the pilot format; the students were exposed to a broad range of techniques and topics which would require numerous diversities to learn on-the-job; a recognition of the importance of this course and the fact that it has been badly needed for a long time; an appreciation for the opportunity to apply tools and techniques mentioned in other courses to real CA problems.

(b)(3)-P.L. 86-36

****
//////////

5. TECHNICAL HEALTH

a. The Z2 Summer Program (Submitted by [redacted] (b)(3)-P.L. 86-36

~~(FOUO)~~ You may have seen the glowing article in the Communicator a couple of months ago about the Director's Summer Program (DSP). You may not be aware that Z2 started its own version of the DSP in 1990.

~~(FOUO)~~ The Z2 Summer Program, like the DSP, is designed to expose gifted math and computer science students to crypto-mathematics. Our program consists of three full-time directors from Z2 and eight to ten students drawn from several different pools. For example, three of our eight students this year are from the Undergraduate Training Program (UTP), one is from the National Physical Sciences Consortium (NPSC) program, one is a math co-op on his third tour at the agency, and the remainder are direct summer hires. Two of our students have been in the Z2 program in past years. Our students are at various academic stages, ranging from two who just completed their freshman year to two first-year graduate students. The students arrived between the middle of May and the first week in June, and they will stay for about 12 weeks. Two facts that apply to all of these students - they are EXTREMELY bright, and they are very enthusiastic about the opportunity to apply math to real problems.

~~(TSC)~~ The Z2 summer program began this year, as it usually does, with some toy problems to get the students comfortable with the computers and with some basic cryptanalytic ideas. Several of our students learned C programming within a couple of weeks. A couple of our returning students were given operational problems to work on at this time, since they required a shorter training period. One of the students quickly became proficient in [redacted] for a particular system. Another pair of students began learning [redacted]

~~(TSC)~~ In early June, we joined the DSP for about seven days of intensive training in crypto-math techniques. (Imagine MA246 and [redacted] crammed into one week!) Following the training period, the students were presented with 14 operational problems, from which they chose their summer projects. About half the problems were diagnosis problems, while the other half were attack development. The students are working in groups of two or three, and most are working on more than one problem. In addition to the accomplishments listed in the last paragraph, the students have in only four weeks completed an [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(FOUO)~~ As you can probably tell, these students are keeping the three of us directors on our toes, and we're learning as much as the students are this summer! If you think you might like to participate in the Z2 Summer Program in the future, you could act as a director (chosen from within Z2), or you could submit a problem and provide technical support for that problem. Feel free to talk to any of us about the program.

[redacted]

(b)(3)-P.L. 86-36

[redacted]

****

b. SPICE - (Background provided by [redacted]

(FOUO) SPICE (Summer Program in Cryptologic Education) is a week-long seminar in advanced mathematical topics. It is given by visiting professors chosen by the leaders of the Agency's mathematical community. The goal is to keep NSA cryptanalysts and cryptologic mathematicians on the cutting edge of technological breakthroughs going on in a variety of specialty areas. Topics in recent years have included: Proving and Discovering Combinatorial Identities, Permutation Polynomials over Finite Fields and Latin Squares, Groebner bases, Modern Permuation Groups and Coding Theory.

(U) This year's SPICE speaker is [redacted] is the designer of the new computer algebra system, MAGMA. In addition to a tutorial, [redacted] will discuss many design and implementation issues which impact the performance of a system like MAGMA. Algorithms for computing in various algebraic structures will also be presented. In particular, algorithms for computing with permutation groups of degree one million will be discussed.

(U) SPICE will be held in the FANX2 Auditorium (see Calendar).8 For further information, contact [redacted] or send a message via e-mail to [redacted]

(b) (6)

(b) (3)-P.L. 86-36

****

c. [redacted]

########## SECOND CALL FOR ABSTRACTS ##########

(SC) CONSCRYPT `94 is being held at GSE from 31 October to 4 November. This is an opportunity to exchange information on targets, cryptanalytic techniques, software development and applications, and trends in communications.

(FOUO) Abstracts, in either flat ascii or framemaker, need to be submitted to [redacted] no later than August 12th. If you have any questions at all, please feel free to call her at [redacted]

****

d. Science & Engineering Society Presentation

(U) The NSA Science and Engineering Society will sponsor a presentation by [redacted] at 1 PM on Tuesday, August 9th in the R&E Symposium Center. [redacted] is the head of the Lincoln Lab Analog Device Technology Group and the principle director of the Consortium for Superconductive Electronics. He will speak on:

(b) (6)

"Advanced Technologies for Signal and Data Processing"

(U) He will describe a variety of analog and digital electronic technologies being developed at the [redacted] This will include silicon based low power analog to digital converters, programmable transversal filters, fiber optic modulators and receivers, superconductor based correlators, compressive receivers

(b) (3)-P.L. 86-36

[redacted]

and directive antennas.

All green and gold badge personnel are invited to attend.

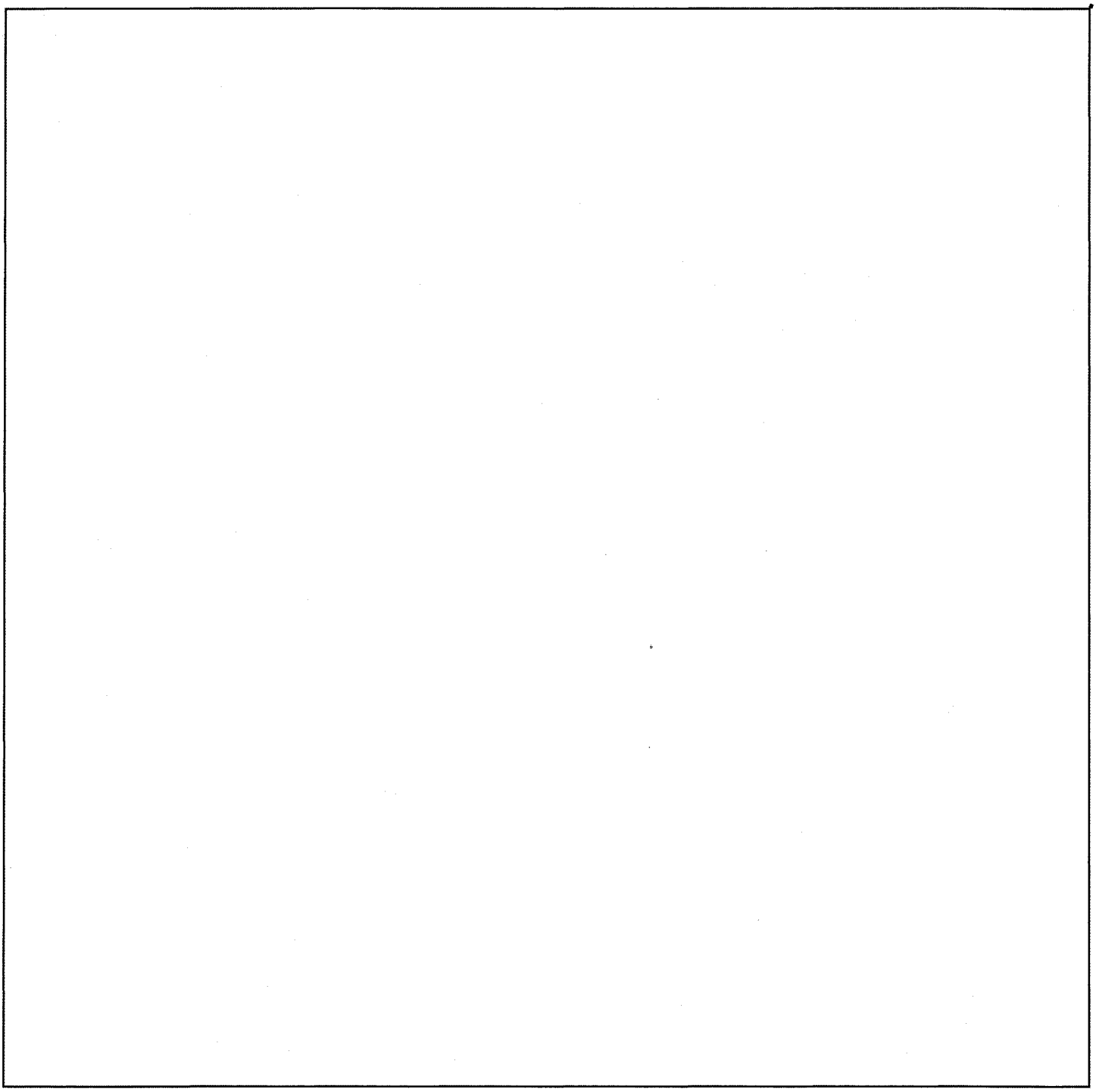
****

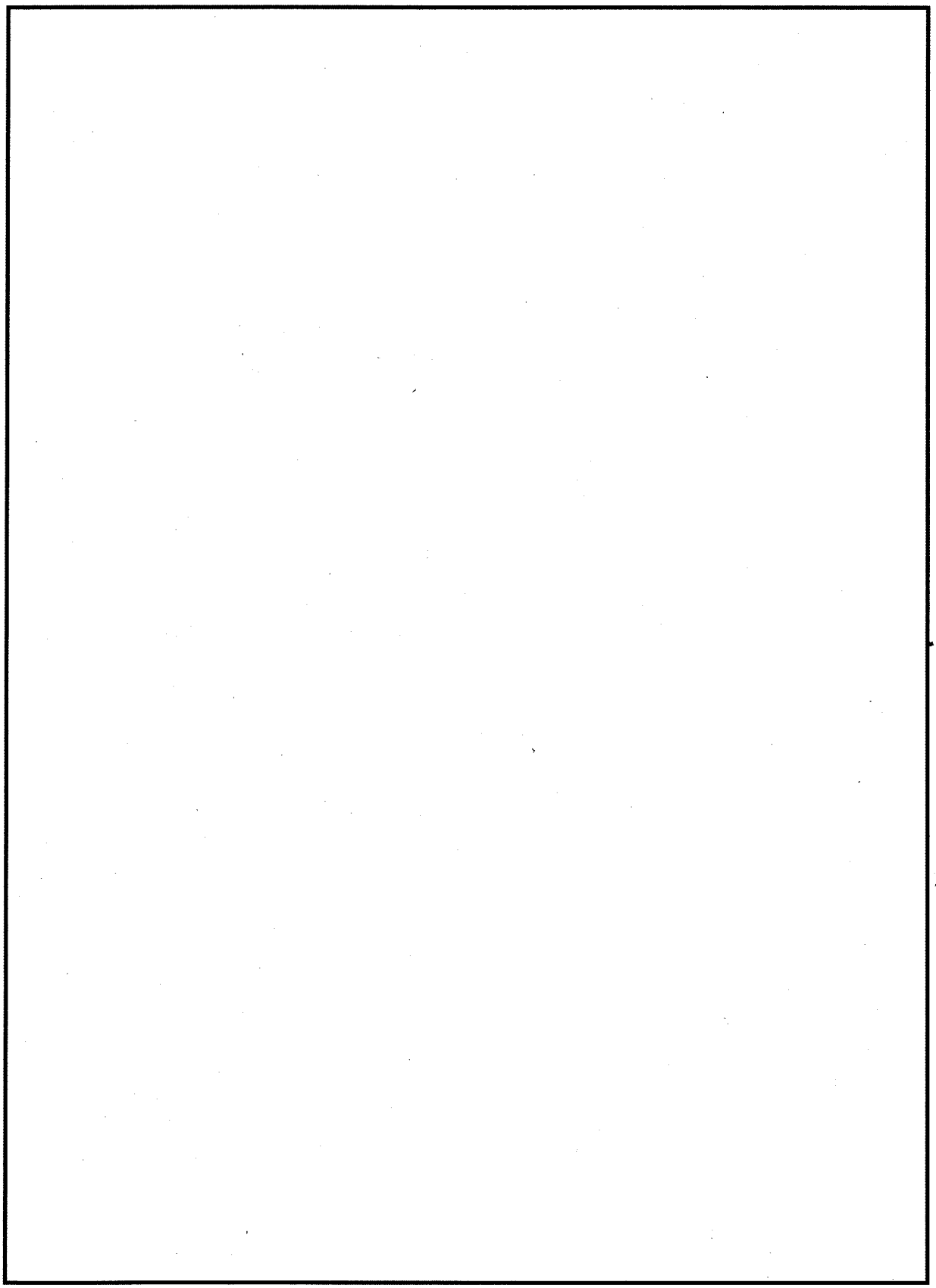
e. ~~(TSC)~~ SOLUTION TO THE JULY PROBLEM OF THE MONTH

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~~~~~~~~~~~~~~~~~~~~~~~ JULY PROBLEM STARTS HERE ~~~~~~~~~~~~~~~~~~~~~~~~

First, let's restate the question for those who missed it.

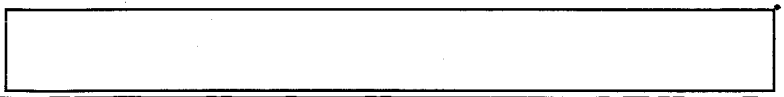

~~~~~~~~~~~~~~~~~~~~~~~~



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

f. AUGUST PROBLEM OF THE MONTH

(b)(3)-P.L. 86-36



[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

****
//////////

6. Technical Topic

Just the Fax (Submitted by [redacted]

(U) You've heard about them, seen them in the local 7-11, and maybe even used them. They are Fax machines and they are as popular as ever with people who want to send a copy of a document anywhere in the world within a few minutes.

(U) Fax is short for facsimile, which is known as telefax in some countries. It is the method by which a page (printed, handwritten, photographic, whatever) is converted into bits, sent via modems over phone lines, and recorded on the other end as a copy. Group 3 Fax is digital in nature (encoded bits are sent with a modem over phone lines) and is the predominant type of Fax used today. Groups 1 and 2 are analog in nature and much older and slower. Group 4 is meant to operate on a digital network instead of regular phone lines.

(b)(3)-P.L. 86-36

(U) Fax is very much like a remote photocopier. One can think of the process of encoding a page of Fax first by taking a picture of the page and converting it into a 1728x1100 raster file (for an 8.5x11 inch page). Each line going down the image is then encoded, usually via a particular Huffman code spelled out by the CCITT standards organization. The encoded bits are then optionally put in error correction packets and/or encrypted and sent to the image modem for transmission. The process is reversed at the receiving end of the transmission to create a raster image which is printed.

(U) Group 3 Fax transmissions are half-duplex and use a 300 bps V.21 modem to send handshaking information, known as T.30 information. To actually transmit an image, a faster modem is used, either a V.29, V.27, or a V.17. The speeds of the image modems range from 2,400 bps to 14,400 bps. To ensure line quality, a 1.5 second burst of all zeros, known as a training sequence, is sent by the transmitter; the receiver will either accept the current speed or request that another training sequence be sent at the next lower speed available. The pages will then be transmitted at the speed which was

[redacted]

accepted by the receiver. T.30 handshaking occurs at the start of a transmission and in between each burst from the image modem.

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) There are those people who say that Fax is a quickly passing fad which will be supplanted by electronic mail, but the evidence so far does not support this theory. A Gallup poll released in April found that the corporate America uses Fax far more than email to the extent that more than a third of telephone bills for Fortune 500 companies are from Fax transmissions. According to the New York Times, the poll found that, "the real appeal of fax machines is that they are easy to use and are an entrenched part of the daily office regimen in a way that E-mail is not." Additionally, pictures, drawings, signatures, and other non-textual information can be easily transmitted via Fax in a way that most email systems cannot handle.

****
//////////

7. Norman Roberts Award - Call for Nominations

(~~FOUO~~) In recognition of Norman Roberts' talent for nurturing the skills of junior analysts, the KRYPTOS Society established the Norman Roberts Award. The award is presented annually to a junior cryptanalyst at NSA/GCHQ who has made an outstanding cryptanalytic contribution.

(~~FOUO~~) Norman joined GCHQ in 1975 and won the respect and admiration of his colleagues for his innovative ideas and particularly for his ability to train and inspire younger analysts up to his untimely death in July 1990.

(~~FOUO~~) Any KRYPTOS member may nominate any employee at NSA or GCHQ who has been at their respective agency for less than five years as of 31 July 1994, and who has made an outstanding contribution to cryptology or a related discipline. The nominee does not have to be a KRYPTOS member. Integrees will be regarded as members of their host agency. The nomination must include the names of the proposer and the nominee, together with an account of the work which attracted the nomination. It may be classified up to TSC. Nominations are due by 1 September 1994 and should be mailed to the KRYPTOS Society secretary, [redacted]

(b)(3)-P.L. 86-36

[redacted]

~~(TSUC)~~ The winner will be selected by a joint UK/USA panel, announced in October and presented with a small engraved plaque.

The winner's name will also be added to a permanent plaque on the first floor in OPS 2B.

//

8. ACTION LINE

a. (U) QUESTION: How are CA Panel members selected? Are there minimum grade levels required? Also, same question about the members of the various committees (paper review, program review, and PQE test committee).

****

(U) ANSWER: (Provided by [redacted] CACP Executive)

The Cryptanalysis Career Panel, the Technical Paper Evaluation Board, the Computer Program Evaluation Board, and the CAPQE Committee are composed of professionally certified Cryptanalysts. The Cryptanalysis Career Panel is a duly constituted board, which means it includes a female representative and a minority representative. The Cryptanalysis Career Panel also includes a military representative. I will list the members of the various Boards below.

The STTB has recently advised that members of the Cryptanalysis Career Panel, and the other career field panels, should come from the GG15, SCE, and SLE ranks. These people are the senior experts in the career field, and probably represent a wide diversity of experience, skills, technical and leadership backgrounds, and have seen the career field grow and change.

(b)(3)-P.L. 86-36

Under normal conditions, the Chairman and members of the Cryptanalysis Career Panel serve three year terms. When the Chairman is two or three months away from the end of his/her term, a list of possible candidates is formed. The Panel starts with the list of certified 15's, SCE's, and SLE's, and also reviews the list of people who have already served on the Panel. Previous experience as a member of the CACP is helpful for the new Chairman, but not a necessity. The CACP forms a short list of candidates in priority order, and the current Chairman then invites each prospective candidate in turn, until one has accepted the position. In the past, the current Chairman was the final selection official, but would not choose a replacement against the advice and consent of the Panel members. When a Chairman is selected, he/she must be approved by DDO, with concurrence by M34.

Panel members are selected in a similar manner, except that the CACP attempts to find representatives from the various areas within cryptanalysis. There are members from different offices in Z Group, and a representative from the NCS.

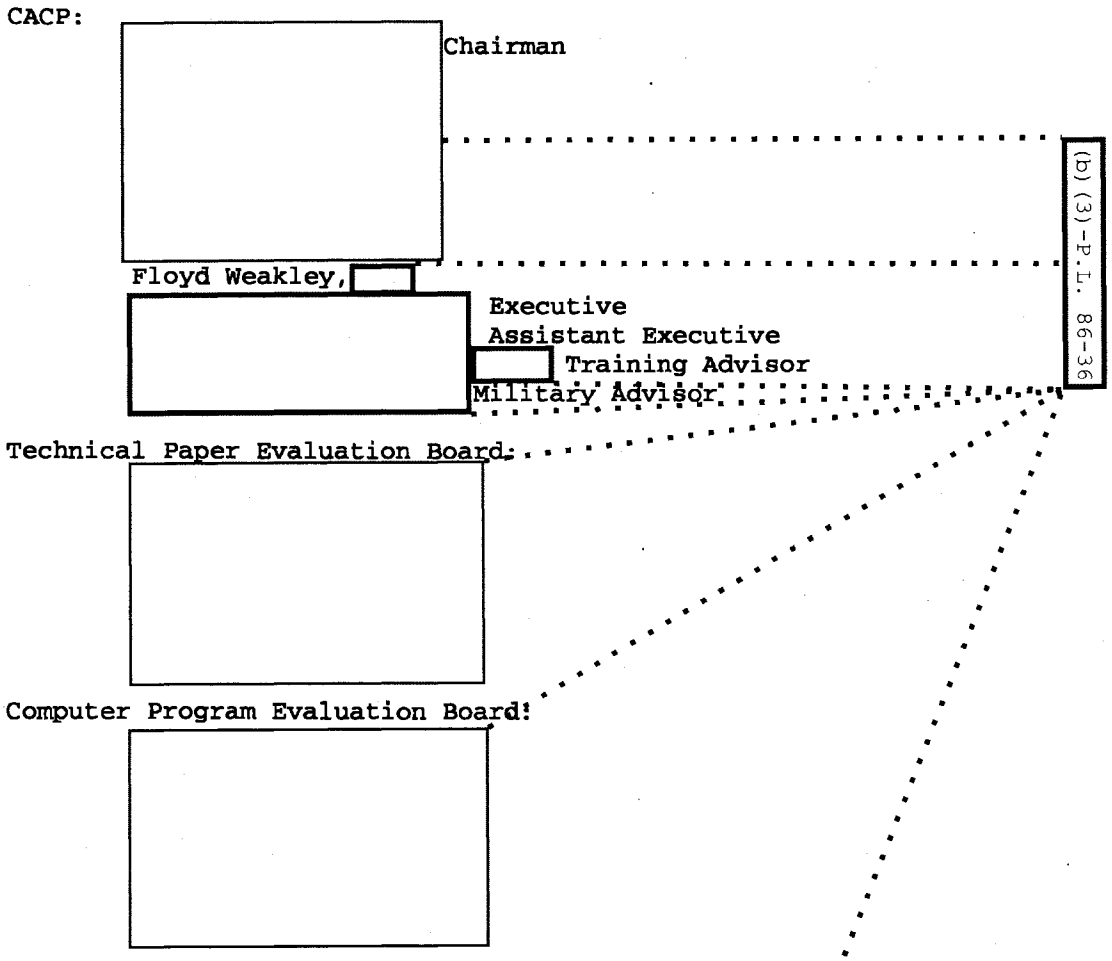
A member of the CACP is also a member of, and acts as liaison with, the Technical Paper Review Board, the Computer Program Review Board, the CAPQE Committee, and the Technical Track Review Panel (TTRP). There is a different liaison to each of the boards/committees/panels. They report back to the CACP at its monthly meeting. Membership on these various boards is by invitation, with the

[redacted]

individual's interest in serving the cryptanalytic community an important consideration for selection. Normally, professionalized cryptanalysts volunteer to be on a board, or are suggested by supervisors, current board members, or current CACP members. A diversity of experience is also an important factor. For example, the current Technical Paper Review Board consists of members from Z1, Z2, Z3, Z4, Z5, and C7. We also try to balance the boards in matters of gender and experience.

Members of the Technical Paper Evaluation Board and the Computer Program Evaluation Board serve terms of about two years, with a staggered rotation schedule, to help maintain consistency and continuity. There are no minimum grade levels for these boards, but members must exhibit technical expertise and competency in the field.

The positions of the Executive and Assistant Executive of the Cryptanalysis Career Panel are advertised through the Agency's Job Vacancy Announcement Process. The selection authority is the Chairman, with the advice of the CACP.



****

QUESTION: A number of people are concerned that, even though it is required that positions at branch level and above be advertised, many of the advertisements appear to be paper exercises only. It seems that selection officials often have a person in mind beforehand. No one wants to spend his time agonizing over whether to apply for a job, inform his supervisor of his intent to leave, and then go to the

trouble of applying IF there is no hope of being selected. At least before, we knew that if we saw an announcement, the office was actually looking for someone. Could someone in Z comment on this, please?

****

ANSWER: (provided by [redacted] Deputy Z, Chair Career Development Board):

I think this an extremely pertinent question which deserves a comprehensive answer. The selecton of managers at the branch level and above is, in my mind, one of the most important responsibilities of the selection official who is usually the immediate supervisor for the position to be filled. It's the responsibility of managers to acquire the resources necessary to carry out their mission and I don't know of any resource more important than the leadership (this is especially true in cryptanalysis where we look more to creative and imaginative problem solving rather than rote solutions which are much more easily managed).

Consequently, there are proactive roles to be played here by both the selecting official and the potential candidates. In my mind it is a gross abdication of a critical responsibility for a selecting official to prepare and publish an advertisement and then wait, in a passive mode, to be presented with a list of candidates from which the selection official will choose! In my experience, I have frequently had to go out and convince a somewhat reluctant candidate to apply for the job. The eventual selection of a heavily recruited candidate may give the appearance that a particular job was "wired" but it certainly doesn't imply that other candidates weren't considered. Fulfilling EEO responsibilities is a critical job element for selection officials who must also extend their proactive role to identifying and recruiting women and minorities who possess the right qualifications.

(b)(3)-P.L. 86-36

In my few short months as D/Z I have seen many jobs advertised and selections made and I continue to be impressed with the professionalism of the selecting officials who really do look over the list of applicants very carefully. I have also observed that several people both in Z and elsewhere in DDO have become increasingly frustrated with a selection process which has repeatedly bypassed them in favor of other candidates. In these cases the perceptions that jobs are "wired" are easily reached. After all, all of us believe we are qualified for the jobs we apply for and may look for explanations why we weren't selected - this is human nature.

I have occasionally seen some shortsightedness on the part of selecting officials and this is where some improvements are possible. A manager will sometimes select someone with recent relevant experience (usually obtained by working within the organization where the vacancy lies) rather than taking a risk on someone unknown to the selecting official who perhaps doesn't see the long term corporate benefits of developing candidates with excellent potential. Here is where selection and advisory boards should play a key role in the process. Recently, we have added an advisory role to the Z group Career Development Board (CDB). Branch and division level management positions are routinely discussed with the goal to cooperatively reach a consensus amongst the selecting official, the office chiefs, and the CDB. Tom Lessard (CH/Z) has endorsed this process.

****
//////////

9. LITERARY TIDBITS

[redacted]

(U) Voynich Manuscript Remains Elusive - (by [redacted]

In Yale's Beinecke Rare Book Collection sits the Most Mysterious Manuscript. Found by Wilfrid Voynich in 1912 in an Italian villa, the book is at least 400 years old. Elegant handwriting fills its pages, as do many anatomical, herbal, and astrological drawings, some in color. Yet, as far as we know, nobody but the author has ever been able to read it.

We don't seem to know enough about the book. The alphabet's size, its origin, and the underlying language are all unknown. Frequency distributions haven't shed much light. Still, some things are known. The book is believed to have been circulating around the court of Emperor Rudolph II of Bohemia during the early part of the 17th Century, and may once have belonged to Rudolph's chief alchemist. Despite the fact that some have attributed the work to Roger Bacon, a 13th-Century Franciscan philosopher and occultist, the author's identity remains a mystery.

Much scrutiny has been given the manuscript. Some people think that it's an elaborate hoax, but the text's structure suggests otherwise. William F. Friedman believed that the "words" were written in an artificial language, in which each letter denotes a different classification for an object (similar to genus and species). In 1928, William R. Newbold presented the first "decipherment," based on an anagramming system so complicated and subjective that practically any interpretation is possible. From the decipherment, Newbold claimed a 13th-Century manuscript origin, with Bacon as author, and argued that Bacon revealed, among other things, his knowledge of 20th-Century astronomy.

Robert S. Brumbaugh, in 1974, claimed that each letter had as many as three plaintext equivalents. Though he holds that the translation has an alchemical flavor, his decipherment technique fails for most of the book. Just a few years ago, Leo Levitov decided that the Voynich alphabet is actually plaintext, that the language is some sort of polyglot, and that the manuscript is a prayer-book for a suicidal cult of Isis. Unfortunately, Levitov's translation is more repetitive than the manuscript seems to be, and provides us with only a few words, which he rearranges without regard to case. In short, nobody has a convincing, accepted translation.

So, the Voynich Manuscript remains a mystery. Any would-be solvers should refer to an Agency publication, "The Voynich Manuscript: An Elegant Enigma" by Mary E. D' Imperio. The Main Library has it; it's the chief source for this article. Yours truly is curious about any recent developments, as well as the cost of photocopies of manuscript pages, and whether some are floating around at the Agency. Decrypted or not, what a great coffee table book it would make!

****
//////////

10. (U) PUZZLE

Here is the solution to last month's puzzle -

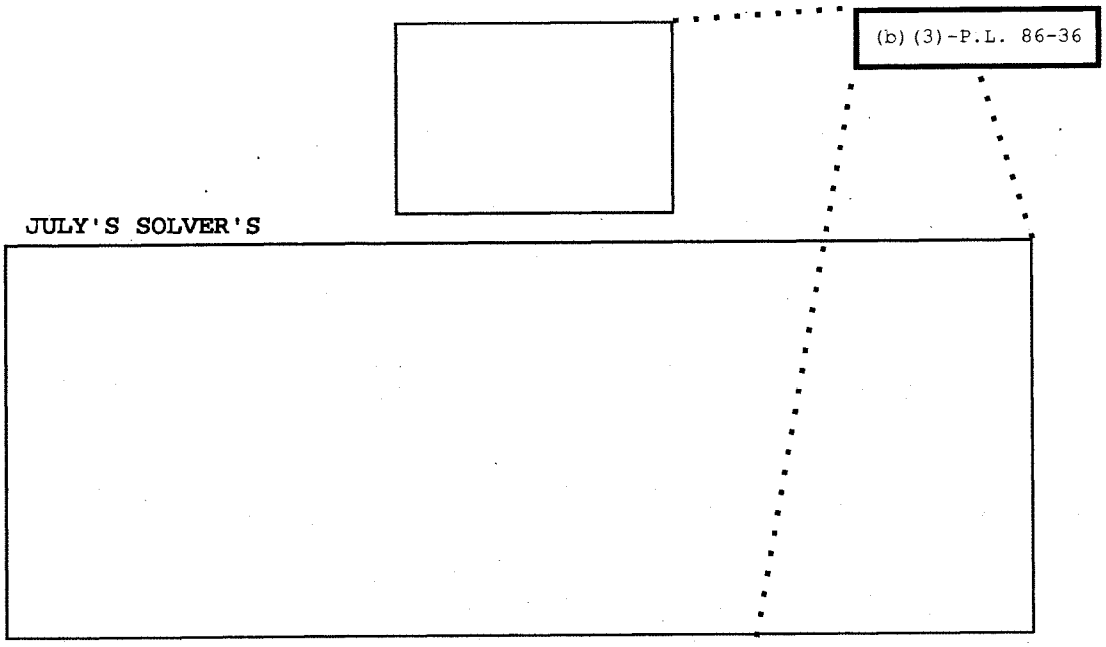
Solution to July Puzzle:

[redacted]

(b) (3)-P.L. 86-36

[redacted]

Doc ID: 6823782

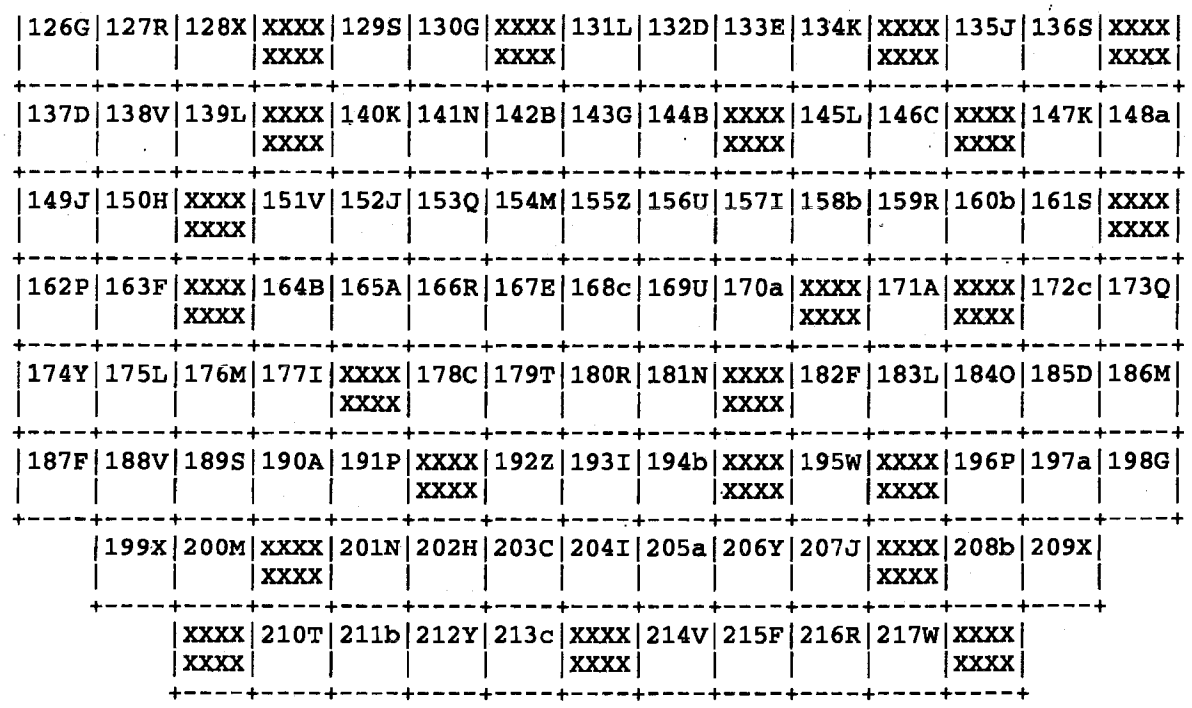


And, for this month, we offer the following - It is not necessary to send your solutions on this one, it is too long. Answer in next month's issue.

"We Knew it All Along!"
by

				XXXX XXXX	1V	2W	3C	XXXX XXXX	4X	5V	6C	7O
8Y	9Q											
10I	11F	12P	13O	14b	15N	XXXX XXXX	16H	17U	18F	19M	20P	XXXX XXXX
21A	22N	XXXX XXXX	23W	24O	25b	26c	27T	28b	29F	30D	31Z	32J
33N	34Y											
35G	XXXX XXXX	36P	37Z	38U	XXXX XXXX	39L	40T	41W	42I	43K	44D	45V
46G	47E											
48R	49J	XXXX XXXX	50O	51H	52X	53a	54H	55C	56R	57U	58D	XXXX XXXX
59A	60H											
XXXX XXXX	61L	62P	63X	64F	65Z	66M	67Q	68T	XXXX XXXX	69K	70W	71K
72N	73X											
74T	75O	76B	XXXX XXXX	77Y	78L	79S	80Q	81B	82N	83J	84a	85P
86E	XXXX XXXX											
87S	88c	89A	XXXX XXXX	90I	91Z	92J	93W	94c	95T	96E	97D	98G
99B	100U											
101R	102M	103E	XXXX XXXX	104O	105U	106D	XXXX XXXX	107E	108c	109H	110K	111S
112A	113Q											
114a	115C	XXXX XXXX	116Z	117B	118Y	119X	120Z	121V	XXXX XXXX	122T	123Q	XXXX XXXX
124B	125H											

(b)(3)-P.L. 86-36



A. ____ ____ ____ ____ ____ ____ ____ Articulated
171 21 165 112 59 190 89

B. ____ ____ ____ ____ ____ ____ ____ ____ Evening song
76 117 164 142 81 99 144 124

C. ____ ____ ____ ____ ____ ____ ____ Vanity
115 178 146 55 3 203 6

D. ____ ____ ____ ____ ____ ____ ____ ____ Estate in Espanol
132 30 185 97 106 44 58 137

E. ____ ____ ____ ____ ____ ____ ____ Pismire palace
133 103 86 167 107 96 47

F. ____ ____ ____ ____ ____ ____ ____ ____ 1 1/3 fluid drams
11 215 187 163 182 18 64 29

G. ____ ____ ____ ____ ____ ____ ____ Fervent
98 198 46 143 130 126 35

H. ____ ____ ____ ____ ____ ____ ____ ____ Flirt
202 60 125 51 150 16 109 54

I. ____ ____ ____ ____ ____ ____ ____ Yacht race
177 204 90 157 193 42 10

J. ____ ____ ____ ____ ____ ____ ____ ____ Small farmers
49 207 135 83 152 92 149 32

K. ____ ____ ____ ____ ____ ____ ____ Layered dessert
147 69 110 140 71 43 134

L. ____ ____ ____ ____ ____ ____ ____ ____ Deception

(b)(3)-P.L. 86-36
9/23/2010

	131	183	145	39	175	78	61	139	
M.									Moor of Venice
	66	200	154	176	19	186	102		
N.									Barren; uninhabited
	15	141	22	82	72	181	33	201	
O.									Rhea's cousin
	184	50	104	24	75	13	7		
P.									Denied
	196	162	62	85	20	36	12	191	
Q.									Locale for a canal
	80	113	153	173	9	67	123		
R.									Extremely serious
	180	216	101	56	159	166	127	48	
S.									Large watchdog
	189	87	161	129	111	79	136		
T.									Flabbergast
	95	74	27	40	179	122	68	210	
U.									Fermat's Little or Last, e.g.
	100	105	57	17	169	38	156		
V.									People
	214	45	151	5	138	188	1	121	
W.									Improve
	93	70	2	195	41	23	217		
X.									Destructive insect
	4	209	199	128	73	52	119	63	
Y.									Cupidity
	118	212	174	77	34	206	8		
Z.									Epithet of Ivan IV
	120	155	37	65	192	116	31	91	
a.									Hurt
	114	205	53	148	197	84	170		
b.									Shipwrecked
	160	14	194	158	211	208	28	25	
c.									A tool in the boot
	172	26	168	108	88	213	94		

****
//////////

11. CONTEST

a. And the winner is..... (b)(3)-P.L. 86-36

[redacted]

(U) Congrats to [redacted] whose proposed title for this newsletter, Tales from the Crypt, received the most votes! Ray wins a double-scoop sundae, and should contact [redacted] to collect same!

(U) Just to let you know, the top five vote-getters were:

Tales from the Crypt - 21
TransCrypt - 15
The CipherSpace - 14
The Kryptogram - 12
Plain & Cipher - 11

(b)(3)-P.L. 86-36

****

b. A NEW CONTEST - What do those vanity license plates mean?

(U) [redacted] has had his vanity license plates, "CURRO26", for over a year now. Although many have tried, no one has succeeded in deciphering it. ([redacted] badgered [redacted] incessantly!)

(U) [redacted] thinks it is so easy that putting it in the new CA newsletter, as a challenge, is an insult to the CA community. He has, however, reluctantly agreed, in view of how intractable it has been. The ground-rules are that respondents will be given only one of two pieces of information - 1) "No, that is not correct" or 2) "Yes, by George, you've got it!"

(U) We will publish the answer next month ONLY IF it is broken, and then the winner (first to submit the correct answer) will win a double scoop sundae from [redacted] Send your guesses to any member of the Editorial Board and we'll run them by him. (We don't know the answer either!)

****

12. EDITORIAL CORNER

If you have a relatively short technical treatise which you think might appeal to our readers, please submit it to any member of the editorial board or any of our office POCs.

(b)(3)-P.L. 86-36

In fact, if you have anything you would like to have considered for inclusion in future issues, please forward it, IN ASCII FORMAT, to one of the POCs listed below. Also, PLEASE paragraph classify each item submitted.

A reminder that anonymity may be requested for Action Line items - in fact, you may mail them in hardcopy form to any member of the editorial board or any of our office representatives.

We would very much like this newsletter to represent a broad cross-section of the CA community - we need some more volunteers to help us, however. Perhaps you would like to work on one of the topics in this issue, or perhaps there is another topic which you think should be included in future issues. Either way, we would like your input, and help, so give one of us a call. The more people who divide up the work, the less burden on any one person.

[redacted]

##
NOTE: We MUST receive any submissions for the September issue by 24 Aug.
##

****

EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum

[redacted] NCS

OFFICE Reps

[redacted]

(b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

(b)(3)-P.L. 86-36

[redacted]

TOP SECRET//COMINT

(C) POC: [redacted] info
(U) *Last Modified: 10/30/2002 11:42:16*
(U)PE EXTERNAL PAGE

****
* TALES OF THE CRYPT *
****

ISSUE 4

September 1994

//

TABLE OF CONTENTS:

(b)(3)-P.L. 86-36

1. Perspectives in CA
   a. Dick Ruhl, D/Ch Z1
   b. [redacted]
2. KRYPTOS Society
   a. Request
   b. Distinguished Members
3. Calendar of Events
4. News from the CACP
   a. New Certifications
   b. 1993 CA Conference Report Update
   c. 1994 CA Conference Call
   d. Biographical Portraits
5. Technical Health
   a. New ESS category for Signals Processing Tasks
   b. CMI September Talk
   c. MEPP Monthly Meetings
   d. FY95 CA and Math Course Schedules
   e. Solution to August Problem of the Month
   f. September Problem of the Month
6. Technical Article
7. Action Line
8. Literary Tidbits
9. Letter to the Editors
10. Puzzle
11. Contest Winner
12. Editorial Corner

//
---

1. PERSPECTIVES IN CA - (We will be asking CA Seniors to contribute their insights. We hope to feature both a Z and a non-Z perspective each month.)

(~~FOUO~~) a. Dick Ruhl, Deputy Chief of Z1

A SENSE OF COMMUNITY

(b)(3)-P.L. 86-36

(U) The key ingredient to cryptanalytic success is people. People with diverse skills. Our best analysts carefully reverse engineer and

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704um)

study the details of each aspect of the entire telecommunications and cryptologic spectrum that impacts on their ability to turn cipher into plaintext. During this period of down sizing and budget reductions we are often reminded that we must be careful to preserve investment capital. Within the cryptanalytic community our investment capital is our people, the infrastructure, and the techniques that have been developed over time. We should realize our strength is in having confidence and trust in our colleagues. We all must convey a sense of priorities and a commitment which allows people to adjust, train and modify our emphasis to those activities which contribute to our infrastructure. The emphasis must be applied even-handedly across the entire spectrum of cryptanalytic functions.

(U) The extended cryptanalysis community at NSA is at the core of many Agency successes. The key ingredient to our success and productivity is people. Historically our analysts become skilled by working on difficult cryptanalytic problems. The ideas generated and the techniques which are then implemented are often generalized and both are constantly improved. To its credit, the cryptanalytic community consistently developed training to teach each successive generation. As technologies changed, the work force adapted and moved forward. Understanding the complexities and weaknesses of new cryptologics, the development of compartmented programs to exploit subtle vulnerabilities, and the willingness to develop intellectual areas of deep technical expertise, which when applied to exploit target communications, have provided the technical leverage to exploit enciphered target communications critical to the U.S. policy makers and in support of U.S. military leaders.

(FOUO) Today's cryptanalyst must be multi-disciplined and have broad experience. As with earlier generations, the cryptanalysts must be problem solvers and have the ability to examine and to determine the cryptanalytically relevant data. For some cryptanalysts, this may mean the mathematics in developing an attack. It might mean developing a linguistic capability. For others the relevant data might be found in

[redacted]

Cryptanalysts must be and have always been willing to acquire in-depth knowledge of related fields impacting on their discipline. This attention to detail and to related fields must continue to be an integral aspect of the cryptanalysts success.

(C CCO) Television and the news media are constantly filled with programs which are being identified and promoted to satisfy the needs of special interest groups. The extended cryptanalytic community has traditionally responded as a community and developed new techniques, new expertise, as our targets and technology have changed. However, traditional is no longer in vogue. We now see a trend toward new programs developing. Each trumpets its claim as a new special interest group. New programs specializing in network attack possibilities or reverse engineering are developing. The energy is focused on the process of setting up these programs with limited access for the work force-at-large. Just the opposite needs to occur. These emerging fields must be open to the Agency analysts who are willing and able to

(b)(3)-P.L. 86-36

[redacted]

adjust. Open to analysts who are currently engaged in these activities and who are striving to obtain practical experience to such a depth that the emerging fields become part of the `traditional' culture. This transition is necessary to preserve the technical health of the community. To solve real problems a cadre of individual experts will be necessary to attack facets of the problem which are too complex for individual specialists. Each must appreciate and recognize the contributions of the other specialists. Given the opportunity I am absolutely positive cryptanalysts will refine their technical skills and develop new pools of experts who can continue to meet the challenges and opportunities that challenge the Agency. Cryptanalysts have developed strong ties with signals analysis and engineering disciplines. [redacted] In each case, the cryptanalytic community has developed depth of technical expertise to interact knowledgeably with other technical specialists and working together these teams have overcome the technology challenge of the moment.

(U) The people I have trusted and encouraged to explore new opportunities have far surpassed my expectations and certainly my own abilities. Our people are our most important ingredient in the development of our community.

(b)(3)-P.L. 86-36

****

(b) Can you believe they did that....

[redacted] (INFOSEC Developmental Security Evaluations)

(~~FOUO~~) One of the joys of cryptanalysis is the occasional feeling of superiority when the analyst sees a mistake by the designer or implementor. In the SIGINT world, we can make money from those unintended designs. That's good, because we in the INFOSEC business have plenty of things that need money to fix! This note is an attempt to share with you the perspectives of one INFOSEC person who grew up as a cryptanalytic mathematician, and who tried to practice cryptanalysis on problems in SIGINT and INFOSEC. The quick summary: INFOSEC uses cryptanalysis every day; finding, assessing, and helping correct the flaws which could harm U.S. interests. To avoid being censored, I'll try to disguise "target nations" in the following. See if you can figure it out.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted] (b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

(U) In addition to signals and "traditional" cryptanalysis, CA opportunities are flooding in from network and system areas. Networked computers pose immense security challenges, and great opportunities for cryptanalysis. "Tools" like signatures and encryption are used; hardware and software protective features like access control lists, audit, and authentication are used. And we in INFOSEC get to pretend we are the hacker, trying to uncover the hidden information with whatever tricks we can find. The problems and opportunities which confront NSA are great - this is a fun time for the problem solver. We in INFOSEC invite you to stop in and chat about your challenges, our challenges, or even your answers to our challenges!

****

2. KRYPTOS SOCIETY

a. REQUEST

(U) We have co-sponsored a fall picnic with the CMI over the last few years, but there seems to be a decided lack of interest this year from the members of both organizations. We would like to know what kind of social activity the CMI and KRYPTOS members would like to have, such as an "end of winter doldrums spring picnic" or a cocktail party, or even a dance. Please take time to let either [redacted] or [redacted] know just what you would like.

b. SPOTLIGHT ON .....
Distinguished Members of the KRYPTOS Society for 1993 (b)(3)-P.L. 86-36

(U) Last fall, KRYPTOS introduced the Society's 1993 Distinguished Members at their annual luncheon. Background on each of the five 1993 Distinguised Members will be featured in the upcoming issues of this newsletter, leading up to the annual luncheon in November.

****

(a). [redacted] (b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(3)-P.L. 86-36
(b)(6)

(U) With the exception of several special projects, [redacted] and its successor organizations. Professionalized both as a mathematician and cryptanalyst, his significant breakthroughs and advances in major research problems over the years merited him a Letter of Commendation from the Director (1970), appointment as a Senior Consultant (1973), the Exceptional Civilian Service Award (1977), an immediate merit promotion by the Director (1978), and a DDO Special Performance Award (1987).

(U) [redacted] demonstrated outstanding performance in a variety of roles - supervisor, research cryptanalyst, and technical consultant. He attended and was a primary participant at many conferences at Princeton and at GCHQ, where he presented technical briefings and led discussion groups of senior analysts and outside consultants. He was a member of many Agency promotion boards and received several Senior Technical Awards. [redacted] last year before retirement was marked by even more impressive successes and a lot of TDY. In 1992, the Director of Central Intelligence awarded him the Outstanding Collector Award.

(b)(3)-P.L. 86-36

... his loss to this branch would be a crippling blow to its research

... responsible for generating ideas, attacks, and hypotheses for all systems

... this achievement is a classic example of cryptanalysis at its very finest

... while an exceptionally brilliant piece of work, it is typical of the work accomplished by him

... has a long history of producing critical cryptanalytic results on a variety of systems

... has a vast store of cryptographic knowledge and an analytic ability second to none.

(b). [redacted]

(U) At the time of her retirement, [redacted] was the Deputy Office Chief of B8. She was a major player in the organizational planning for and creation of Z Group. An exceptional mathematician and cryptanalyst, she spent the majority of her career performing analytic and technical leadership functions of increasing complexity and importance. She distinguished herself by producing the finest ever annual report on the status of cryptanalysis and putting together a related briefing for the Director.

(b)(3)-P.L. 86-36

(U) [redacted] communications skills were quite evident. She

[redacted]

authored a variety of technical papers, taught courses, and was an active and eloquent participant at SCAMP and cryptanalytic research conferences. Her papers and notes were used in the development of several cryptanalytic courses.

(U) [redacted] wrote increasingly complex software and made fundamental improvements to widely used diagnostic attacks. Her technical liaison talent was often used to bridge the gap between cryptanalysts and the programmers or engineers who were developing support systems. Her ability to clearly articulate the need in a way that could be understood by outsiders was remarkable. She was the cohesive factor in coordinating complex cryptomathematical research against a broad variety of sophisticated systems.

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36
(b)(6)

(c). [redacted]

[redacted]

(U) During his five years at the National Cryptologic School, [redacted] developed CA-107, Exploitation of Manual cryptosystems; taught CA-260, Diagnosis and CA-301, Bookbreaking; originated and directed CA-305, Annual CA Seminar; and served as Chief of the CA Division. He then became Executive of the Cryptanalysis Career Panel. During his tenure as Executive, he oversaw the growth from less than [redacted] to more than [redacted] interns and built a stronger program, largely by allowing interns greater participation. Morale improved through the publication of a newsletter, intern meetings, and a brochure for new hires. [redacted] practiced TQM before it was fashionable. He also designed the CA Technician Program and helped to form the KRYPTOS Society.

[redacted] can best be characterized by the following comments:

* extraordinary level of honesty, integrity, and enthusiasm
* extremely sensitive to personal and career needs of the work force
* inspired junior analysts to persist in attacking challenging problems
* flexible, willing to help out wherever he was needed
* excellent interpersonal skills
* outstanding breadth of knowledge
* left a strong legacy by his outstanding leadership

(b)(3)-P.L. 86-36

c. (S) We have extended the deadline for nominations for the Norman Roberts Award to the 15th of September. As a reminder, this award is presented annually to a junior cryptanalyst at either NSA or GCHQ who has made an outstanding cryptanalytic contribution. "Junior" has been defined as on who has been at his/her respective Agency for less than

[redacted]

five years as of 31 July 1994. While there is some on-going discussion about this definition, it will be followed this year. Any KRYPTOS member may nominate any employee, Nomination must include the name of the nominee, the nominator, and a write-up of the work which attracted the nomination. It may be classified up to TSC. Please mail to the KRYPTOS secretary, [redacted]

****

3. CALENDAR OF EVENTS

UPCOMING

Sep 7	MEPP Brown Bag Lunch and Movie (2B5038, 1200-1300)
Sep 8	CMI - "Modern Results on an Ancient Problem" (0930, Friedman) (See 5b)
Sep 8	HRMA Roundtable Discussion on "Networking for Career Development", 2C086, 1100-1230)
Sep 8	"Stress - Is it Worth Dying for For?" (Movie, 1100, 3W083)
Sep 12	Z Technical Forum Talk - Asynchronous Transfer Mode (ATM), by [redacted]
Sep 12	"Stress - Is it Worth Dying for For?" (Movie, 1100, 2C086)
Sep 15	Norm Roberts' Award Nominations Due - (see 2c)
Sep 15	Flexible Employment Plan (FEP) Open Season Ends
Sep 19-20	Healthy Heart Mini-Fair (OPS1 N. Cafeteria, 0715-1030, Call 688-3400 to register)
Sep 19-21	Cryptanalytic Computing Conference (SRC)
Sep 20	Security Day "The Steven Lalas Espionage Case - presented by the FBI (Friedman, 1000 & 1300) Tickets available in 1S079.
Sep 23	"Stress - Is it Worth Dying for For?" (Movie, 1100, 3C086)
Sept 26	Pen and Cursor Society - [redacted] on Writing got Profit (0930-1100, 9A135)
Sep 27	International Affairs Institute (IAI) Talk "Intelligence Sharing Worldwide", (1030-1130 Ambassador Montgomery, OPS2B, Rm 2B4118-6)
Oct 7	TSP Workshop (0900 Friedman)
Oct 13	IAI Talk "Nuclear Missile Proliferation", (9A135 1030-1130, Larry Gershwin, NIO S&T)
Oct 17-21	[redacted]

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

Oct 19-21	ESCAPE `94 (Biennial ciphony experts' conference) - NSA
Oct 31-Nov 4	CONSCRYPT at CSE
Nov 4	KRYPTOS Luncheon (Officers' Club)
Nov 7-10	Data Demodulation Workshop (FanxII)

PLAN AHEAD:

March 27-31, 1995	CARD (GCHQ)
May 15-19	CA-305
May 34-35, 1995	CA PQE

//

4. WORD FROM THE CACP -

a. (FOUO) Congratulations are in order for the following people who just completed their CA professionalization!

[redacted]

b. (FOUO) The Report from this year's CA Conference is on the streets! Copies were sent to all those who participated, and also sent in hard copy to Distro IV (down to Branch level). The report contains the full text of the keynote addresses and working group reports, and gists of the technical briefings. Tapes are available for the entire conference proceedings, and may be viewed in the CACP office, or may be borrowed for viewing elsewhere. If you have not seen the report and would like to have a hard copy, please contact either [redacted] or call them at [redacted] (secure). Future issues of this newsletter may carry parts of this report, space permitting.

(b) (3) -P.L. 86-36

c. (FOUO) The CACP has already begun to think about next year's Conference, which will probably be held again at SRC in January 1995. They are open to suggestions for topics and/or themes, and ask that you forward any suggestions to [redacted], or any panel member.

d. (U) BIOGRAPHICAL PORTRAIT (Each month we will introduce one or two of the most recent people to have joined either the CA Intern program or the CA Tech Program. In the future we may also include interviews with some of the more senior members of the CA community.)

[redacted]

(b)(3)-P.L. 86-36

1. ~~(S)~~ [redacted] is a first-tour intern assigned to Z421, working first on the [redacted] and now on the [redacted] in addition to learning to program and attending the many classes required by the intern program.

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

2. ~~(S)~~ [redacted] is a first-tour intern currently assigned to Z433. She is working on the [redacted] including [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(FOUO)~~ Before entering the intern program [redacted] worked in [redacted] the Office of Policy. She was a Freedom of Information Act Case Officer. As such, she was responsible for responding to requests for information about NSA from the public. She searched the Agency for responsive information and applied exemptions to this information before releasing it to the requester.

~~(FOUO)~~ Having worked in DDO for about five years before going to DDP, [redacted] recalled that she really enjoyed the TA aspects of her job. She was "really interested in getting back into analytical work." [redacted], her division chief, brought the CACP's intern vacancy announcement to her attention and encouraged her to apply.

(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

(b)(3)-P.L. 86-36

[redacted]

[redacted] (b)(3)-P.L. 86-36 (b)(6)

****
//////////

5. TECHNICAL HEALTH

a. New ESS category for Signals Processing Tasks (b)(3)-P.L. 86-36

(FOUO) [redacted] is the author of a set of Cray-based programs for performing signals processing tasks. Recently he obtained an ESS category (#1433), which he will use to notify users in advance of changes or new programs. Following is a brief description that Ed provided to us. (b)(1) (b)(3)-P.L. 86-36

[redacted]

b. CMI September Talk - (see calendar for date/time, etc.) (b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

(TSC) Double transposition is one of the oldest cipher systems that still poses difficulties for the cryptanalyst. [redacted]

[redacted]

c. MEPP Monthly Brown Bag Lunches - [redacted]

(U) The Math Education Partnership Program, an outreach effort for improving math and science education in grades K-12, will hold monthly luncheon meetings, on the first Wednesday of each month, for its volunteers, beginning this month. This will be an opportunity to share ideas, sees movies or hear talks about other initiatives, etc. This month there will be a movie about an innovative teacher of math in Harlem. It is very entertaining and full of wonderful ideas for interacting with students. After this motivating movie there will be a discussion of what it means to be a member of the Speakers' Bureau. Future meetings and agenda will be announced on ESS, #1393, so please subscribe if you are interested. Questions? Call [redacted] (b)(3)-P.L. 86-36

d. Course Schedules - [redacted]

Following is a listing of [redacted] FY 95 schedule for Cryptanalysis and Cryptomathetics courses. Changes to this schedule tend to occur fairly often (usually due to circumstances beyond our control!). We'll make every effort to announce such changes, as soon as they become

[redacted]

known, on Enlighten, admin.training. If you have any questions, please give us a call on 968-7051.

NCS CLASS SCHEDULE IN COURSE DESIGNATOR ORDER
FOR CA COURSES
(PERIOD COVERED 941001-950930)

DESIG CL-FY

START/STOP	SESSION	DAYS/HOURS	ROOM

CAD01 01-95 SPEECH ANALYSIS — DEPT: E42 SIZE: 024
950104-950106 1 WF 1300-1500 A2B058 FANX2
950109-950210 2 MWF 1300-1500 A2B058 FANX2
ALLOC: Z(18) R(1) H2(5)
INSTR: STAFF

CA015 01-95 INTRO TO MANUAL & MACHINE CRYPTOSYSTEMS — DEPT: E42 SIZE: 011
941128-941216 1 DAILY 0800-1600 A2324 FANX2
ALLOC: A(2) B(4) H2(2) I(1) K(1) V(1)
INSTR: [redacted]

CA015 02-95 INTRO TO MANUAL & MACHINE CRYPTOSYSTEMS — DEPT: E42 SIZE: 011
950703-950721 1 DAILY 0800-1600 A2328 FANX2
ALLOC: A(1) B(4) H2(2) K(1) V(1) Z(1) ARMY(1)
INSTR: [redacted]

CA101 01-95 GENERAL CRYPTANALYSIS FOR MATHEMATICIANS — DEPT: E42 SIZE: 018
950905-950929 1 DAILY 0800-1600 A2B024 FANX2
ALLOC: Z(16) C(2)
INSTR: STAFF

CA104 01-95 INTRODUCTION TO CRYPTOLOGY AND NSA — DEPT: E42 SIZE: 010
950103-950120 1 DAILY 0800-1600 A2328 FANX2
ALLOC: B(1) V(2) Y(1) Z(4) HQAIA(2)
INSTR: STAFF

CA110 01-95 INTRODUCTORY CRYPTOSTATISTICS — DEPT: E42 SIZE: 009
950306-950317 1 DAILY 0800-1200 A2324 FANX2
ALLOC: C(1) H2(3) J(1) M(1) N(1) Z(2)
INSTR: STAFF

CA110 02-95 INTRODUCTORY CRYPTOSTATISTICS — DEPT: E42 SIZE: 009
950807-950818 1 DAILY 0800-1200 A2328 FANX2
ALLOC: C(1) H2(2) R(1) Z(3) M(1) N(1)
INSTR: STAFF

CA112 01-95 [redacted] — DEPT: E42 SIZE: 011
941011-941031 1 DAILY 0800-1600 A2324 FANX2
ALLOC: Z(7) H2(4)
INSTR: STAFF

CA112 02-95 [redacted] — DEPT: E42 SIZE: 011
950103-950124 1 DAILY 0800-1600 A2324 FANX2
ALLOC: Z(8) H2(3)
INSTR: STAFF

CA112 03-95 [redacted] — DEPT: E42 SIZE: 011
950403-950421 1 DAILY 0800-1600 A2324 FANX2

[redacted]

(b)(3)-P.L. 86-36

ALLOC: Z(7) H2(4)
INSTR: STAFF

CA112 04-95 [redacted] DEPT: E42 SIZE: 011
950703-950721 1 DAILY 0800-1600 A2324 FANX2
ALLOC: Z(8) H2(3)
INSTR: STAFF

CA123 01-95 SHIFT REGISTER CRYPTOLOGY DEPT: E42 SIZE: 016
941003-941110 1 DAILY 0830-1100 A2B058 FANX2
ALLOC: C(2) H2(3) J(1) N(1) R(1) V(4) W(1) Y(1) Z(2)
INSTR: [redacted]

CA123 02-95 SHIFT REGISTER CRYPTOLOGY DEPT: E42 SIZE: 016
950313-950331 1 DAILY 0800-1600 A2B058 FANX2
ALLOC: C(2) H2(3) J(1) M(1) N(1) R(1) V(3) W(1) Y(1) Z(2)
INSTR: [redacted]

CA123 03-95 SHIFT REGISTER CRYPTOLOGY DEPT: E42 SIZE: 015
950807-950915 1 DAILY 0830-1100 A2B058 FANX2
ALLOC: A(1) C(2) H2(3) M(1) R(1) V(3) Y(3) Z(1)
INSTR: [redacted]

CA207 01-95 COMPUTER APPLICATIONS FOR CRYPTANALYSIS DEPT: E42 SIZE: 008
950522-950602 1 DAILY 0800-1600 A2328 FANX2
ALLOC: H2(2) Z(4) F6(2)
INSTR: [redacted]

CA219 01-95 ADVANCED CRYPT ANALYTIC TECHNIQUES DEPT: E42 SIZE: 010
941128-941216 1 DAILY 0800-1600 A2328 FANX2
ALLOC: H2(3) Z(7) INSTR: STAFF

CA219 02-95 ADVANCED CRYPT ANALYTIC TECHNIQUES DEPT: E42 SIZE: 010
950217-950217 1 F 0800-1600 A2328 FANX2
950221-950310 2 DAILY 0800-1600 A2328 FANX2
ALLOC: H2(3) Z(7)
INSTR: STAFF

CA219 03-95 ADVANCED CRYPT ANALYTIC TECHNIQUES DEPT: E42 SIZE: 010
950501-950519 1 DAILY 0800-1600 A2328 FANX2
ALLOC: H2(4) Z(6)
INSTR: STAFF

CA223 01-95 INTERMEDIATE SHIFT REGISTER CRYPTOLOGY DEPT: E42 SIZE: 016
950103-950210 1 DAILY 0830-1100 A2B058 FANX2
ALLOC: C(7) H2(3) J(2) K(1) R(1) Z(2)
INSTR: [redacted]

CA223 02-95 INTERMEDIATE SHIFT REGISTER CRYPTOLOGY DEPT: E42 SIZE: 016
950710-950728 1 DAILY 0800-1600 A2B058 FANX2
ALLOC: C(6) H2(4) J(2) W(1) R(1) Z(2)
INSTR: [redacted]

CA235 01-95 MACHINE ANALYSIS FOR MATHEMATICIANS DEPT: E42 SIZE: 025
950306-950421 1 MWF 0900-1100 A2B024 FANX2
ALLOC: C(6) Z(19)
INSTR: STAFF

CA250 01-95 KEY GENERATION SYSTEMS DEPT: E42 SIZE: 011
950313-950428 1 MWF 0800-1100 A2328 FANX2

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

ALLOC: Z(10) H2(1)
INSTR: [redacted]

CA261 01-95 DIAGNOSTIC WORKSHOP DEPT: E42 SIZE: 010
950206-950217 1 DAILY 0800-1600 A2324 FANX2
ALLOC: H2(2) Z(8)
INSTR: [redacted]

CA301 01-95 CRYPTOLOGY OF CODES DEPT: E42 SIZE: 011
941017-941104 1 DAILY 0800-1600 A2328 FANX2
ALLOC: H2(5) Z(2) OPEN(4)
INSTR: STAFF
CA301 02-95 CRYPTOLOGY OF CODES DEPT: E42 SIZE: 011
950424-950512 1 DAILY 0800-1600 A2324 FANX2
ALLOC: SPECIAL(11)
INSTR: STAFF

CA323 01-95 ADVANCED SHIFT REGISTER CRYPTANALYSIS DEPT: E42 SIZE: 012
941017-941104 1 DAILY 0800-1600 A2B038 FANX2
ALLOC: C(1) H2(1) Z(7) F6(1) OPEN(2)
INSTR: [redacted]

CA323 02-95 ADVANCED SHIFT REGISTER CRYPTANALYSIS DEPT: E42 SIZE: 012
950605-950623 1 DAILY 0800-1600 A2B038 FANX2
ALLOC: C(1) H2(1) Z(8) F6(1) OPEN(1)
INSTR: [redacted]

(b)(3)-P.L. 86-36

==========

MA148 01-95 INTRO TO CRYPTO MATHEMATICS FOR MATHEMAT DEPT: E42 SIZE: 024
941011-941215 1 TR 1300-1500 A2B024 FANX2
ALLOC: Z(20) H2(2) R(1) OPEN(1)
INSTR: STAFF

MA204 01-95 ALGEBRAIC CODING THEORY DEPT: E42 SIZE: 024
950306-950511 1 MWR 1300-1500 A2B024 FANX2
ALLOC: Z(19) C(5)
INSTR: STAFF

(b)(1)
(b)(3)-P.L. 86-36

MA213 01-95 [redacted] DEPT: E42 SIZE: 024
941024-941202 1 MWF 0900-1100 A2B024 FANX2
ALLOC: Z(20) C(2) H2(2)
INSTR: STAFF

MA246 01-95 CRYPTOMATHEMATICS FOR MATHEMATICIANS DEPT: E42 SIZE: 020
950103-950210 1 DAILY 0800-1600 A2B024 FANX2
ALLOC: Z(16) C(2) H2(2)
INSTR: STAFF

MA250 01-95 THEORY OF LINEAR RECURSIVE SEQUENCES DEPT: E42 SIZE: 024
950626-950901 1 MWF 0900-1100 A2B024 FANX2
ALLOC: C(4) K(6) R(1) W(4) Z(7) F6(2)
INSTR: STAFF
MA256 01-95 SIGNAL PROCESSING MATHEMATICS DEPT: E42 SIZE: 024
950403-950526 1 MWF 0900-1100 A2B058 FANX2
ALLOC: Z(18) C(5) OPEN(1)
INSTR: STAFF

MA302 01-95 FOURIER ANALYSIS DEPT: E42 SIZE: 024
950731-951006 1 MWF 1300-1500 A2B058 FANX2
ALLOC: Z(18) C(5) OPEN(1)

[redacted]

INSTR: STAFF

MA414 01-95 COMBINATORIAL MATHEMATICS DEPT: E42 SIZE: 024
950711-950831 1 TR 0900-1100 A2B024 FANX2
ALLOC: Z(18) C(5) OPEN(1)
INSTR: STAFF

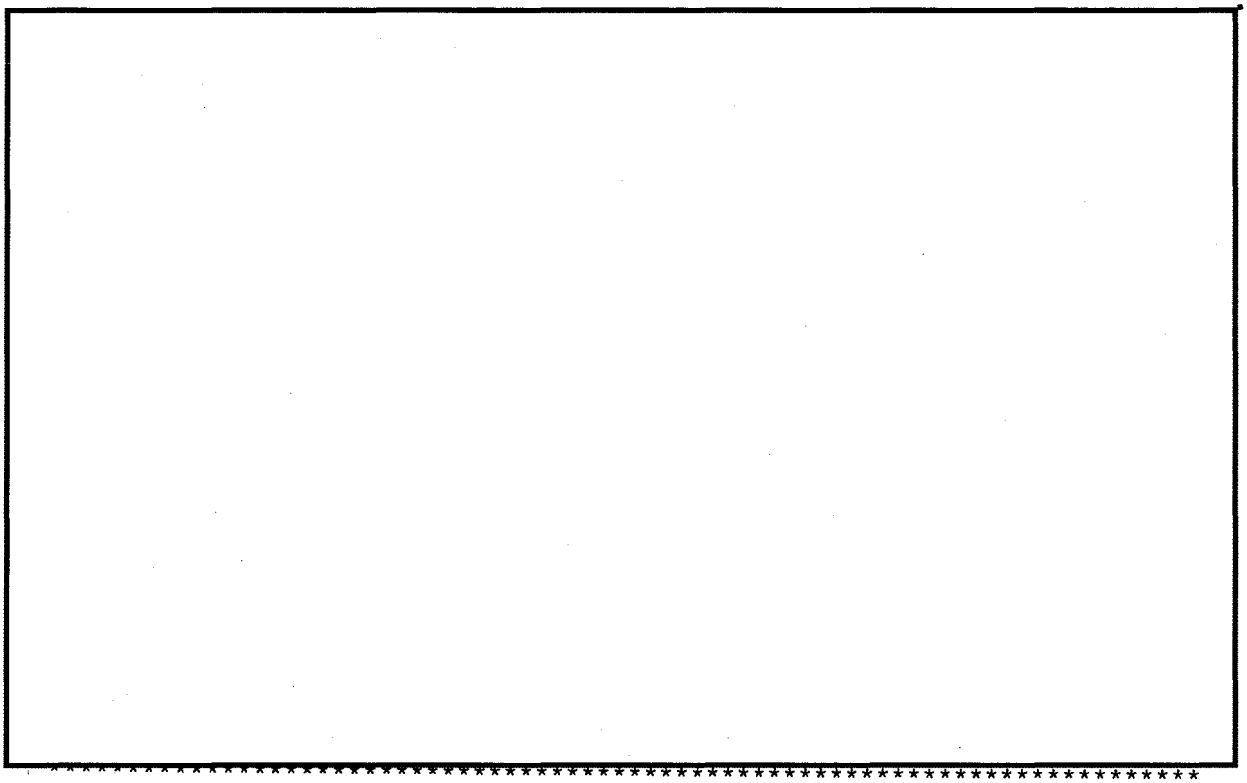
MA550 01-95 NUMBER THEORY FOR CRYPTOLOGY DEPT: E42 SIZE: 024
950403-950623 1 MWF 1300-1500 A2B058 FANX2
ALLOC: Z(18) C(5) OPEN(1)
INSTR: STAFF

"""""""

f. September Problem

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~TOP SECRET UMBRA~~



6. Technical Topic

ARITHMETIC COMPRESSION

(U) Arithmetic compression is a relatively new technique which provides excellent data compression but with the cost of processing time which is far greater than that used by other compression schemes. Unlike other techniques, arithmetic compression explicitly relies upon a well-designed language model to provide estimates for upcoming characters and then derives its compression from the roughness in the estimates. Arithmetic compression has not caught on for text compression due to the expense of computation but it will soon become a critical part of compression schemes for both color and black and white images.

(b)(3)-P.L. 86-36

(U) To illustrate how arithmetic compression operates, take an alphabet consisting of four characters A,B,C,D with corresponding probabilities .5, .25, .125, and .125. We begin with two values, HIGH = 1.0 and LOW = 0.0 and we will recompute values of HIGH and LOW as we step through the message. Think of A as owning the bottom half of the line segment between LOW and HIGH (i.e., from 0.0 to .50), B owns the next quarter(.50 to .75), C the next eighth (.75 to .875) and D the last eighth (.875 to 1.0). We choose the new HIGH and LOW values to be the boundaries of the line segment owned by the first character of the message. So if B is the first character of the message we would have HIGH = .75 and LOW = .50. We now subdivide this new line segment according to the probabilities of the characters (A now owns the segment from .50 to .625, B from .625 to .6875, etc.) and repeat the

process for the next character of text. When all the text has been processed, the compressor publishes the midpoint of the final region (LOW,HIGH). To decompress, one must be able to track the procedure which created the midpoint. That is, at each step of the process the decompressor needs to know which of the four possible line segments, corresponding to the four characters of the language, contains the midpoint in question. It is not hard to show that if the compressor publishes the first -log(HIGH-LOW) + 2 bits of the midpoint then the decompressor has sufficient information to complete the job. It can also be shown that, on average, the value -log(HIGH - LOW) represents the best compression possible for messages which satisfy the given list of probabilities. With the probabilities given above, the message BAADA would yield values HIGH = .55859375, LOW = .5546875. The midpoint is .556640625 and the compressed text is 100011101. The nine bits of compressed text are only slightly better than one would have gotten by simply assigning two bits to each character, but for longer messages we would expect the compressed text to average 1.75 bits per character.

(U) Now, a few details have to be worked out. The most obvious problem is that we are using decimals which need to become increasingly more precise and thus we seem to need to use a multi-precision package to do the computations. In fact, what happens is that the high order bits of HIGH and LOW soon become equal so that the high order bits of the ultimate output become fixed. The compressor can output those bits and keep the remaining bits in a single register. Also, our example had a static language model; that is, the probabilities for the characters were constant from time to time. But there is no reason why the probabilities can't be recomputed after each step of the compression since the decompressor is capable of performing the same calculations. Several text compressors have been written which use sophisticated language models to select the character probabilities. In general these compressors will produce shorter output than other compression techniques but they are usually much slower because the language modelling is time-consuming.

(U) There is one application of arithmetic compression that is soon to become important. When encoding binary data several tricks can be used to speed up the computations involved in modelling and compression. Two international standards groups, JPEG and JBIG, have been considering a form of arithmetic compression for image compression. JPEG has recommended binary arithmetic compression as an option for the compression of color images and JBIG is working on a standard for the compression of black and white images which will require arithmetic compression. It is likely that future generations of facsimile machines will work according to the JBIG standard.

****

7. ACTION LINE

a. (U) Question: How was the voting membership of the CA TTRP decided? What safeguards are in place to ensure an equitable representation from all areas of Z? Is there a minimum amount of breadth and depth of CA experience necessary to be a member of the CA TTRP? What are the requisite qualifications for CA TTRP membership?

****

(U) Answer provided by [redacted] Chairman of the CA TTRP - (b)(3)-P.L. 86-36

[redacted]

(U) The original CA TTRP was established via a "jumpstart group" policy designed at the DDO level. Several prominent Cryptanalysts were asked to surface a list of candidates for the first panel. The jumpstart group also titled the first panel, based on the criteria that had been developed by the CA Panel. These criteria were developed in conjunction with all of the other included skill fields represented in the new Agency Technical Track, at a series of meetings of the Senior Technical Track Board (STTB).

(U) The original (and current) panel was selected, not to "ensure representation" from areas of Z, but to be composed of bona fide cryptanalysts who could be relied upon to make fair determinations of their peers, regardless of assigned organization. No minimum requirements were officially set, but the first group chosen were those who would be seen as Master level cryptanalysts by the community.

(U) Since the original panels for all skill fields were formed, the additional requirement of being "duly constituted" with minority and female representation has been added, and the CA TTRP has complied. From the start, the CA TTRP has been concerned with equitable representation - but for the applicant, and not to present a superficial allotment by organization. The Panel is concerned with genuinely being fair, not just appearing to be.

(U) Rest assured that all title applications are carefully reviewed, and further researched if there is insufficient first hand knowledge of an individual among the panel members. Also keep in mind that most senior cryptanalysts have worked in a variety of organizations and frequently have a good knowledge of an organization, its people and special expertise, though they may not work there at the moment.

****

8. LITERARY TIDBITS (Review by [redacted]

(b)(3)-P.L. 86-36

How To Tell the Liars from the Statisticians
by Robert Hooke

Why would a statistics consultant, former manager of Mathematics at Westinghouse, a fellow of the American Statistical Association, and member of the Operations Research Society of America write a humorous book on statistics? Why would you want to read one?

Many people are scared away from "mathematics" even though they unknowingly deal with mathematics, especially statistics, in many areas of their lives. This book gives anecdotal evidence to support statistical techniques and their usefulness to the average American (however you want to define "average" or "American").

In 76 one- to three-page chapters, Dr. Hooke hits on such varied topics as "Are You Average Enough?", "Who is Unemployed?", "Things to Think About While Waiting to See the Doctor", "Zero or Nothing?", "More is Less", "Watch Out for 67%", and "There Are No Easy Solutions". (The last one is something to keep in mind on election day!) In addition to making complex statistical techniques and terms understandable and applicable to everyday living, Dr. Hooke helps the reader regain (or learn) enthusiasm for statistics.

[redacted]

Chapter 39, Scaling Up and Down reminds us that rules that apply to things that are small don't always apply to those that are big. "If you can solve a two-piece jigsaw puzzle in two seconds, it doesn't follow that you can solve a 3000-piece puzzle in 3000 seconds (fifty minutes)." In our Agency careers we will see many reorganizations; the most recent will not be the last. Why so many? Dr. Hooke helps define the "whys" of reorganization: "Sometimes the change is made for purposes of decentralization, ... In other cases the change glorifies consolidation, ... All of this reorganizational activity is a crude way of trying to reach an optimal position where the trade-offs of big vs. little are as profitable to the corporation as possible. If corporations remained quali[ta]tively the same as they grew, there would be no need for such activity."

If you are interested in other such nuggets, and a very readable, enjoyable book, look for "How to Tell the Liars from the Statisticians" in the NSA Library, call number QA276.12.H66, in the Enhanced Mathematics Collection.

****

9. (U) LETTER TO THE EDITOR (From [redacted]

I read with interest the CA Panel's response to the Z4 Survey Briefing. While I agree with most of the response I feel that it contained some mis-perceptions, as well as a somewhat patronizing tone. Foremost, the statement that this effort was intended to "lower the standards of excellence" for judging cryptanalysts is absolutely false. In fact, their proposal was designed to try to influence the CA criteria to include aspects that would help make it germane to the communications and other changes in our targets that we are facing in Z4. The response encouraged movement away from specialization toward flexibility. I certainly agree; to be successful the cryptanalysts in the production offices must learn to deal with collection problems, data forwarding issues, garbled traffic, changing requirements, etc. They must constantly interface with reporters, linguists, collection managers, signal analysts, other cryptanalysts and mathematicians. Flexibility must be their middle name! But nowhere in the CA criteria are these traits really addressed. Related Fields is not even a part of the examination anymore.

One other comment I would like to address is that cryptanalysts should not stay in a single office for long periods of time. This is a noble statement and it is certainly true that mobility is desirable for both gaining and sharing experience. But it is a fact of life that many cryptanalysts, including those outside Z4, do not readily move from office to office. And many of them are our most productive employees, and often among the most well-rounded. If the community is serious about such diversity, it should be institutionalized. We have lots of interesting problems in Z4 that could use fresh ideas from, for example, Z2 or Z5 experience.

[redacted] all certified professionals, recognized a problem and made a good faith effort to both quantify the extent of feelings about the issue and present possible solutions. They spent a great deal of their own time working at this, and they should be commended for their commitment. Hopefully they have raised the consciousness of the community, but I'm afraid that the tone of the panel's response will only stifle similar "grass roots" efforts to

(b)(3)-P.L. 86-36

[redacted]

bring forth perceived problems.

To repeat, I basically agree that our professional cryptanalysts should be well-rounded in the CA disciplines. This means training, diversity tours, seminars, conferences, etc. Programming skills, problem- solving traits, and the ability to communicate, orally and on paper, are important. It really is an individual's responsibility to do whatever is necessary to become certified. However, it is not asking too much for the CA community itself to consider whether their criteria is relevant to much of their constituency, or perhaps could use some fine-tuning, as several other disciplines have done.

****

10. (U) PUZZLE

Here is the solution to last month's puzzle -

"The mathematical tools of cryptanalysis are continually subjected to rigorous analysis, refinement and generalization. The intrinsic beauty is equal to that of any field in pure mathematics. As [redacted] once proclaimed, "It's a great science we have here!"

[redacted] CRYPTOLOGIC MATHEMATICS

A. JOINTED	K. PARFAIT	U. THEOREM
B. SERENADE	L. TRICKERY	V. HUMANITY
C. CONCEIT	M. OTHELLO	W. ENHANCE
D. HACIENDA	N. LIFELESS	X. MEALYBUG
E. ANTHILL	O. OSTRICH	Y. AVARICE
F. TEASPOON	P. GAINSAID	Z. TERRIBLE
G. ZEALOUS	Q. ISTHMUS	a. INJURED
H. COQUETTE	R. CRITICAL	b. CASTAWAY
I. REGATTA	S. MASTIFF	c. SPANNER
J. YEOMANRY	T. ASTONISH	

****

(b)(3)-P.L. 86-36

And this month we bring you .....

EQUATIONS
by [redacted]

Each equation below represents a phrase, fact or title which contains the given number. For example:

3 = M and a B would be "Three Men and a Baby"
9 = I in a B G would be Nine innings in a baseball game

[Warning for solvers at GCHQ, CSE and DSD: this puzzle has a definite bias towards U.S. culture (and no, that is not an oxymoron :-). However, in the interests of international peace I've taken out some (but not all) of the worst offenders. (Of course you already knew that it was 897 steps to the top of the Washington Monument, didn't you?) You're welcome. -Larry]

1	=	F O the C N	18	=	W on a T-T
1	=	W on a U	24	=	B B in a P
3	=	B M (S H T R)	24	=	H in a D
3	=	S to the W	26	=	L in the A

[redacted]

4	=	F of P on M R	29	=	D in F in a L Y
4	=	F of M I	31	=	F of I C at B R
4	=	Q in a G	32	=	D F at which W F
6	=	L on an I	40	=	D and N of the G F
6	=	P in a P T	40	=	C on a C B R
6	=	W of H the E	54	=	C in a D (with the J)
7	=	V of S	57	=	H V
7	=	S in the B D	64	=	S on a C B
7	=	W of the A W	66	=	B of the B (K J V)
8	=	S on a S S	76	=	T that L the B P
8	=	N in an O	80	=	D to G A the W
9	=	P in the S S	88	=	P K
10	=	L I	90	=	D in a R A
11	=	P on a F T	101	=	D
12	=	A M	200	=	D for P G in M
12	=	L of H	206	=	B in the H B
12	=	S of the Z	1000	=	W that a P is W
13	=	S on the A F	1001	=	A N
14	=	D in a F	1215	=	Y the M C was S
16	=	O in a P	1760	=	Y in a M
18	=	H on a G C	20000	=	L U the S

****

11. CONTEST - [redacted] Vanity Plates

(U) And the winner is [redacted] now of N51, but a former member of the NCS CA faculty. Sharon is an obvious Latin scholar, as she correctly translated 'CURRO' as 'I run'. [redacted] is a marathon runner; ergo, I RUN 26! Sharon gets a sundae from Joe! We had one other correct guesser, [redacted] of Z3, and about 15 other guesses, some quite creative, and even close to the mark!

(b)(3)-P.L. 86-36

****

12. EDITORIAL CORNER

If you have a relatively short technical treatise, or anything you would like to have considered for inclusion in future issues, please submit it to any member of the editorial board or any of our office POCs.

PLEASE paragraph classify each item submitted, and USE ASCII FORMAT!

A reminder that anonymity may be requested for Action Line items - in fact, you may mail them in hardcopy form to any member of the editorial board or any of our office representatives.

We would very much like this newsletter to represent a broad cross-section of the CA community - we need some more volunteers to help us, however. Perhaps you would like to work on one of the topics in this issue, or perhaps there is another topic which you think should be included in future issues. Either way, we would like your input, and help, so give one of us a call. The more people who divide up the work, the less burden on any one person.

##########
NOTE: We MUST receive any submissions for the October issue by 23 Sep.
##########

****

EDITORIAL BOARD

[redacted]

[redacted]

Jack Ingram, Cryptologic History Museum

[redacted]

OFFICE Reps

[redacted]

(b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

[redacted]

TOP SECRET//COMINT

~~(C) POC:~~ [redacted] *info*
(U) *Last Modified: 10/30/2002 11:42:16*
(U)PE EXTERNAL PAGE

(b)(3)-P.L. 86-36

****
* TALES OF THE KRYPT *
****

October 1994

//
##

WE ARE LISTENING ..... (Note from the Editorial Board)
.....

(U) We have received lots of very favorable comments on our first four issues, and we thank you. Our only somewhat negative feedback has been on the length of the issues. We have been somewhat inundated with articles and announcements, etc., which obviously reflects the need for such a publication, BUT, we also want everyone to read the entire newsletter! SO, we have listened to your suggestions, and have made a few cuts. We will only do one Senior CA Perspective each month, and one interview of the new Interns, CA Techs, etc. We also will only include the answer to the puzzles, so if you want the puzzle, save it for yourself.

##

****CHALLENGE*****CHALLENGE*****CHALLENGE*****CHALLENGE*****CHALLENGE*****

(U) The challenge this month is from the Editorial Board. We have changed something. First person to e-mail the correct answer to [redacted] gets an ice-cream sundae.

##
//

(U) TABLE OF CONTENTS:

1. Perspectives in CA - [redacted] 2. KRYPTOS Society
   a. More 1993 Distinguished Members b. Announcement re KRYPTOS Talks 3. Calendar of Events 4. Word from the CACP
   a. New Certifications b. CA Panel Changes
   c. 1994 CA Conference Update
   d. Biographical Portraits
5. Technical Health
   a. Z Tech Talk Info
   b. Want Ad
   c. New Language and Linguistic Rersource Center
   d. Science and Engineering Gociety Presentation
   e. Problem of the Month
6. Technical Article
7. Community Service
   a. American Cryptogram Association & Bulletin Board Service
   b. Apples Needed
   c. Cryptologic Almanac

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

d. National Crypt Museum
e. Math Speakers Bureau
8. Open Letter to the CA Community
9. Literary Tidbits
a. "Decrypting ISBNs"
b. Crypt History in the First Person
10. Action Line
11. Puzzle
a. Solution to "Equations"
b. Arbor Day
12. Editorial Corner

//

1. ~~(FOUO)~~ PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice, alternating between Seniors from within Z and Seniors outside Z. This month we are pleased to print the thoughts of [redacted] regarding

CHANGE: IT'S PART OF OUR LIFE

~~(FOUO)~~ I welcome a chance from the editors of Tales of the Krypt to give my perspective on a CA topic. The topic I chose is change and how it has affected me in particular and why I like it. All opinions are mine and are based on my experiences.

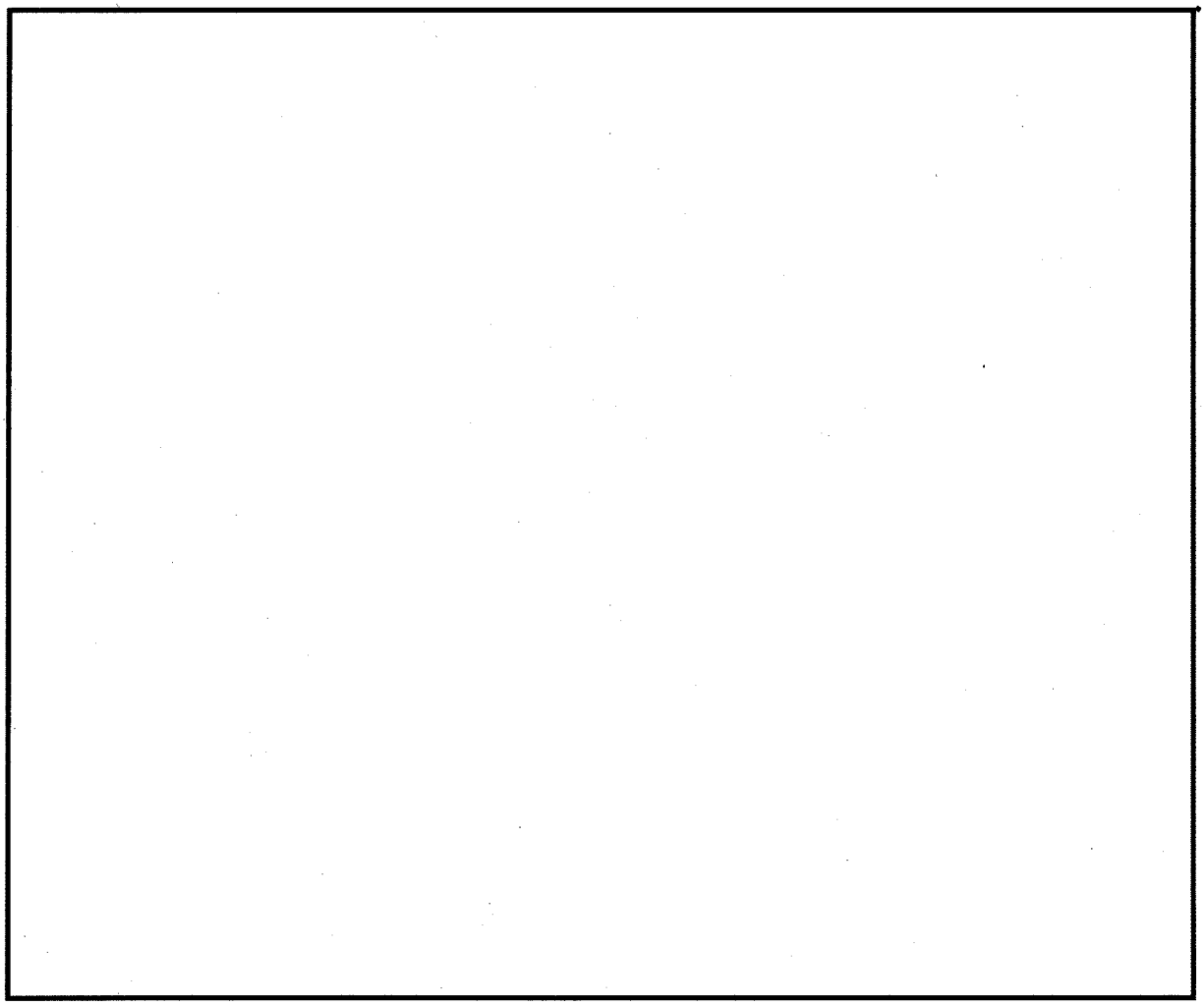
~~(S-CCO)~~ When I graduated from the P1 program (now called the CMP program) I had to decide on a permanent assignment. As for most interns this choice was not easy for me. I had had several very interesting tours and each organization I considered had a lot to offer. In the end I made my selection of [redacted]. The deciding factor in my choice was change. To me, both [redacted] worked on problems for long periods of time. The problems were fascinating, but were very much long-term(i.e. not much change). [redacted] appealed to me because the problems changed and I felt I was better suited to work on their problems. I did not have the patience or stick-to-itiveness [redacted] So early on in my career I decided that I liked change. Little did I know how much change I would get!

(b) (3)-P.L. 86-36

[redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[redacted]



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(TSC) In summary, my entire Agency career has been affected by changes in the cryptology [redacted]. For the most part this change has produced a plethora of interesting problems, many of which I have been able to work on. I expect to continue to be affected by change for the rest of my career. I just hope I enjoy the coming change as much as I have enjoyed the change I have already seen.

(b)(1)
(b)(3)-P.L. 86-36

//

2. (U) KRYPTOS SOCIETY

a. 1993 Distinguished Members (continued)

MAHLON DOYLE

Mahlon Doyle hails from North Baltimore, Ohio. After serving three years in the U.S. Army at the Pentagon and in Manila during World War II, he pursued his education at George Washington University, earning an A.B. in Mathematics, a B.E.E. in Electrical Engineering, as well as doing graduate work in mathematics there and at American University.

Mr. Doyle began his NSA career in 1949 as a cryptanalyst and progressed from cryptologist to mathematician to Branch Chief to Division Chief in Cryptomathematics. He became a Senior Cryptographer in 1976 and currently holds that title in the Office of Information

(b)(3)-P.L. 86-36

[redacted]

Security Research and Technology. Among the awards he has received are: Cryptographic Literature Award, Exceptional Civilian Service Award, Distinguished Member of the Crypto-Mathematics Institute, and the National Intelligence Community Citation/National Intelligence Distinguished Service Medal. Mr. Doyle has written over 130 papers on cryptologic topics, including original work in theoretical and applied mathematics; cryptographic design and design principles; cryptanalysis and cryptanalytic techniques; and historical papers describing the evolution of the science of cryptology.

[redacted] has a long list of articles to his credit in such learned publications as the Journal of Algebra, the Digest of the Society for Information Display, and the Annals of Math Studies. Among his published articles are: [redacted]

(b) (6)

b. KRYPTOS Talks

(U) We are in the process of establishing a collection of tapes of previous KRYPTOS talks. This collection will be catalogued, and housed in the Z Tech Library. We expect to have this completed within the next month, and will keep you informed. If you have any of these tapes currently in your possession, please send them to [redacted]

//

3. ~~(FOUO)~~ CALENDAR OF EVENTS

UPCOMING

Oct 6	CMI TAlk (0930 Friedman) "Mathematicians Turn Chips into Logs" [redacted] (b)(3)-P.L. 86-36
Oct 7	TSP Workshop (0900 Friedman)
Oct. 11	NSA Science and Engineering Society Talk 1000, R&E Symposium Center - (see Tech Health)
Oct 13	IAI Talk "Nuclear Missile Proliferation", (9A135 1030-1130, Larry Gershwin, NIO S&T)
Oct 17	Z Technical Forum - Asynchronous Transfer Mode [redacted] (1300-1400, OPS1 3S040) - (see Tech Health)

[redacted]

(b) (1)
(b) (3)-P.L. 86-36

Oct 17-21 [redacted]

Oct 19-21 ESCAPE `94 (Biennial ciphony experts' conference) - NSA

Oct 31-Nov 4 CONSCRYPT at CSE

Nov 3 CMI TAlk (0930 Friedman)
"SCAMP 1994"
[redacted]

Nov 4 KRYPTOS Luncheon (Officers' Club)

Nov 7-10 Data Demodulation Workshop (FanxII)

Nov 11-12 MD/DC/VA Section of the MAA Fall Meeting
Western Md College

Nov 14-Dec 12 Health Benefits Open Season

PLAN AHEAD:

Jan 24-25, 1995 1995 Cryptanalysis Conference (SRC)

March 27-31, 1995 CARD (GCHQ)

May 15-19, 1995 CA-305

May 23-25, 1995 CA PQE

//

4. (U) WORD FROM THE CACP -

a. There are four new professional certifications in Cryptanalysis:

[redacted]

(b) (3)-P.L. 86-36

b. The following CACP members have completed their terms:

[redacted] Chairman, will be replaced 1 November by [redacted]

[redacted] Military Advisor

[redacted] Training Advisor, is replaced by [redacted]

c. ~~(FOUO)~~ Update on the 1994 Cryptanalysis Conference Report submitted by [redacted]

(b) (3)-P.L. 86-36

Many of you have now seen the report from the 1994 Cryptanalysis Conference which was sponsored by the Cryptanalysis Career Panel in January of this year. On the second day of that conference, the attendees were split into five groups and sent off for the better part of the day to address a specific topic. In the next few issues of "Tales of the Krypt", we would like to bring you up to date on the status of the recommendations made by those working groups. Since I was a moderator for one of the working groups

[redacted]

and I am also on the editorial board of this newsletter, it seemed natural that I should "volunteer" to do the first segment. (b)(3)-P.L. 86-36

[redacted] and I were the moderators of the working group tasked with looking into the topic of "Marketing CA". Our group saw our problem to be a three-fold one. We needed to improve the communication within our community, to educate upper level management (above Z) as to what we do and how the Agency benefits from it, and to assure that our customers know what our needs and capabilities are. Points two and three are related. Our customers include the TOPIs, other cryptanalytic offices working the same target, and upper level management.

The easiest place to start seemed to be within our own community. Since the Cryptanalysis Career Panel and the Kryptos Society are the two main organizations concerned with the health of Cryptanalysis, it was suggested that they form a partnership with the intent of improving communication within the community. It was thought that a monthly newsletter should be published in order to facilitate the spreading of information, and more frequent Kryptos talks would be good for our technical health. Members of these two organizations did get together and the result is the publication of this newsletter. Additionally, a member of each organization attends the meetings of the other. As far as there being more Kryptos talks, we're working on that. This cannot be achieved without volunteers from within the Cryptanalysis community. (Call or e-mail the Cryptanalysis Career Panel or any member of the Kryptos Council to volunteer to give a talk or to suggest a topic for a talk that you would like to see presented.)

Cryptanalysts are sometimes hurt because we are thought of as enigmas by many members of promotion boards above the Z level. For this reason, name recognition is even more important for us. One way to improve this situation is to publicly reward those who excel in our field. While we have defined a number of prestigious awards for our career field (among them the Gold Bug and Peter Marychurch Awards), there is a need for more. As a community, we do not adequately publicize either the availablility of these awards or, worse yet the recipients. There was also thought to be need for more team awards. The Cryptanalysis Career Panel responded to this by defining a new Gold Bug Team Award; the names of the first recipients were engraved on a plaque installed in OPS #2B and were published in a previous issue of this newsletter. Kryptos has also recently defined a new award for community service, the Peter Jenks Service Award. The August issue of this newsletter carried a small article on the Norman Roberts Award and solicited the community for nominations.

Many outside of our community also believe that cryptanalysts are mathematicians and that mathematicians are cryptanalysts. This is often, but not always, the case. There are many among us without a degree in mathematics and there are a number of mathematicians out there who have no real feel for cryptanalysis. Our group believed that we need to educate those who make the decisions about hiring. We would like some say in whom we hire to replenish our field. While we realize that it is unlikely that we will be able to bring in anyone in the near future who does not have a degree in a "critical" field, we would like to be able to request that some of the mathematicians that are brought in have a strong background in another field also, such as a foreign language, art, history, or political science. Such a two-fold nature is characteristic of many of our best crytpanalysts. While hiring is currently at an all time low, there are on-going discussions about hiring into the Cryptanalysis Intern Program.

Another suggestion made by the group was to set up an infrastructure designed after the 15-minute OP INTEL Briefings that are currently given to

(b)(3)-P.L. 86-36

DDO and the Office Chiefs. We believe that these briefings do serve the purpose of informing the upper level managers outside of Z about the successes attained by cryptanalysts. It was thought that the original OP INTEL briefings could be taped and shown to the Z workforce, a similar series could be given to Branch and Division level management, and a third set could be directed towards the TOPIs.

We have made some progress on this. In May 1994, a series of monthly Z INTEL briefings began. The audience consists mainly of Division level management and above, but there is sometimes room for people at the branch level. No one has addressed the broad topic of communication with the TOPIs. On a local level, the divsion where I work (Z22) has been doing "target review" sessions with their counterparts in Z4 and with the OPIs. It seems to me that this idea could catch on.

d. (FOUO) Biographical Portrait

[redacted] came to NSA as a CA intern about nine years ago. Having completed the professionalization requirements in her first five tours, she was able to go to [redacted] for her last tour. Recalling how much she had enjoyed teaching in graduate school, [redacted] was eager to try it again. During this tour, she taught MA-146 and CA-110, and wrote a text for CA-110.

Upon graduation from the intern program, [redacted] where she worked on the [redacted] signals which she had worked during two of her intern tours. She thoroughly enjoyed her work there, staying two years.

Her next assignment was in [redacted] where she worked four years. Her primary responsibility in [redacted] was course development. She was also responsible for revising CA-110 to incorporate classified applications from MA-145 and MA-146; teaching CA-110 and CA-123; writing a text for CA-104/105; and coordinating the development of CA-112. She further enjoyed the opportunity to work on the CA Job Task Analysis evaluation committee, serve on the PQE committee, act as the math liaison for the MA courses taught by adjunct faculty, and serve as the E42 coordinator for this year's offering of SPICE.

During her tenure in [redacted] was appointed the CACP training advisor, acting as the liaison between the career panel and the NCS. As training advisor, [redacted] attended panel meetings as a non-voting member to report on any current training issues, then reported any concerns raised at the meeting to the school through [redacted]

"Being the training advisor is a great opportunity for someone in the school to become familiar with the sorts of issues discussed by the career panel," [redacted] says, "and to maintain a sense of continuity with that field." When [redacted] in September to work in [redacted] the training advisor position was filled by [redacted] As is true for all CA instructors, [redacted] adds that she is sure [redacted] would welcome any input on training issues.

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

5. TECHNICAL HEALTH

[redacted]

a. (~~FOUO~~) Z Tech Talk Info: (b)(3)-P.L. 86-36

[redacted] Technical Talk on the 17th of October will focus on Asynchronous Transfer Mode (ATM), a new technology for high speed transmission of mixed types of digital data.

b. (U) Want Ad:

The Math Speakers Bureau is looking for a Female Role Model volunteer to give a presentation on cryptology/cryptanalysis to 7th grade girls at Montgomery Blair High School for a Females in Science and Technology Seminar on Saturday, November 12, 1994. If anyone is interested please let me know as soon as possible.

For further info, contact [redacted]. To volunteer to help, please contact [redacted] or [redacted] (One other person has volunteered so far.)

(b)(3)-P.L. 86-36

c. (U) New Language and Linguistic Resource Center

According to the CLARION, the Cryptolinguists' Association (CLA) newsletter, the new Language and Linguistic Resource Center has just opened. It resides in room [redacted] and the hours are approximately 0630-1600 (depending on the availability of personnel). Their holdings include dictionaries, grammar books, magazines, newspapers, and audiotapes in over a hundred different languages. There are also books on a variety of other subjects such as language teaching and linguistics. There is an on-line database to help you find what you need. They are always looking for donations of language-related material, and they offer a freebie shelf for their extras. The POCs are [redacted] and [redacted]

(b)(3)-P.L. 86-36

d. (U) Science and Engineering Society Presentation

The speaker for our October 11, 1994 Symposium at 1000 will be [redacted] will speak on Statistical Methods for Human Language Systems. This will include applications to speech recognition, machine translation and text understanding.

(b)(6)

[redacted]

e. (~~TSC~~) PROBLEM OF THE MONTH

Apparently, the Problem of the Month for last month has not been solved. Therefore the problem is being extended another month. Please mail all solutions to the editor of the Problem of the Month, [redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted] This Problem of the Month was designed to be a little more difficult than previous problems. As a result, it is expected that you may need a computer to solve this and future Problem of the Months. As a hint, it is suggested that you may want to run some programs from the [redacted] Also, the user of this system has been known [redacted] If you don't have the cipher, it can be found in the last Tales of the Krypt in org.kryptos on ENLIGHTEN. Let [redacted] hear how you are doing!

6. (U) TECHNICAL ARTICLE (b)(3)-P.L. 86-36

WHAT IS A CRYPTOLINGUIST?

by [redacted]

Don't ask Webster, for he apparently has no clue. Were he to include a definition for this term in some future edition, however, it might read something like this:

Cryptolinguist \'krip-to-'lin-gwest\ n [Gk kryptos + L lingu- + L -ista] 1: One who is expert in a language and uses that knowledge to solve codes and ciphers (see cryptogram) 2: An obscure profession which required intense concentration and mental intensity, the practitioners of which were all killed off by Muzac during the late 20th century.

So here we have a term that is a combination of Greek and Latin, a mixture of fire and water, an amalgamation of hope and despair. The wanton death and widespread destruction precipitated by the four Macedonian Wars between 215 and 148 B.C. are all wrapped up in this single obscure word. And yet there remain those who wonder why we few remaining cryptolinguists are looney, or at least appear to be so!

To expand the definition of the term CRYPTOLINGUIST as it applies to the real, everyday efforts expended by those who claim that title, we must note that the CRYPTO portion means "cryptanalysis" which Webster does recognize and describes simply as "the solving of cryptograms or cryptographic systems," while the LINGUIST portion means, in our usage, a "language expert" or a person adept in one or more target languages. It is essential to recognize that the prefix CRYPTO modifies the base word LINGUIST and thus a CRYPTOLINGUIST is a type of linguist, not a type of cryptanalyst. To define CRYPTOLINGUIST then, we need to relate how such an animal differs from another type of linguist.

We recognize four essential elements that are necessary for one to be an effective CRYPTOLINGUIST. These can be assigned the acronym LIFE.

1. LANGUAGE: The single most essential element and the only one that can be accomplished (at least to a certain level) via formal training. The more familiar the CRYPTOLINGUIST is with the target language, the more successful he or she will be in breaking codes. Also, better language skills facilitate the acceleration of one's development in the remaining three essential elements.

2. INSIGHT: The ability, often developed over years of practice, to see the "big picture" through the fog of scattered letters and/or digits. This insight can range from the microscopic recognition of digital patterns to the macroscopic realization of parameter (b)(3)-P.L. 86-36

limitations. One who has developed such insight can combine one's intense knowledge of the target language and sense, even with a paucity of evidence, that the subject code messages are based on a dictionary, a novel, a manufactured chart, or any other variation.

3. FLEXIBILITY: While a CRYPTOLIGUIST can learn much from that which has gone before by studying the work of colleagues and maintaining comprehensive notes, lists and charts of data from his or her own earlier efforts, flexibility is a key attribute. One's mind must be constantly challenged and open to avoid the tendency to force round pegs in square holes. Unlike the actuary or accountant who knows a given amount of rules and formulas, some combination of which must apply to a given set of data, the CRYPTOLINGUIST must be always alert for something new and different. He or she must be flexible enough to recognize the constant changes and obscure developments which characterize code construction. All the rules and formulas for the CRYPTOLINGUIST have never been written nor will will they ever be.

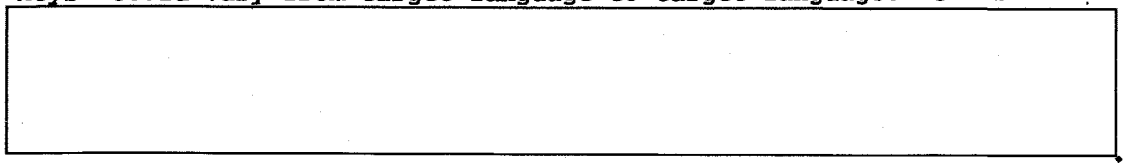
4. EXPERIENCE: An on-going stockpiling of information and techniques that enhance one's abilities in the first three attributes. This is, thus, perhaps the most sigificant attribute of all. Such experiences can be manifested and solidified by the CRYPTOLINGUIST who concentrates on the three keys that make a truly superior practitioner. These three keys employ the acronym MID.

   a. Memory: The ability, for example, to see a certain pattern among the lines of characters and equate it to a similar one studied perhaps years earlier. We note that there have been some very good CRYPTOLINGUISTS who couldn't remember what day it was, but the really superior CRYPTOLINGUIST develops a good memory and improves it as he or she progresses through a lengthy career.

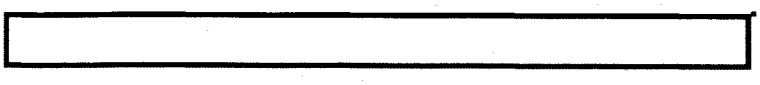
   b. Identification: The most successful CRYPTOLINGUISTS also engage in Traffic Analysis and in-depth research on their target. To try to recover a code system without any knowledge of the target creates a lot of questionable recoveries such as those for organizations, etc. Developing a full understanding of the target enhances the CRYPTOLINGUIST'S efforts.

   c. Documentation: Some CRYPTOLINGUISTS feel that they are code-breakers only. They have neither the time nor inclination to document their findings. A year later, that person has been re-assigned and another CRYPTOLINGUIST is given the problem which must be started from scratch. Documentation not only maintains continuity and assists others in picking up the dropped ball, but it certainly helps the documenting CRYPTOLINGUIST because it forces him or her to identify the entity, it helps in memorizing patterns, and it greatly enhances experience.

We would be remiss if we did not here admit that the relative import of each of the "four essential elements" and the "three keys" could vary from target language to target language. Codes in



(b)(3)-P.L. 86-36



9/23/2010

We have thus defined the attributes of a true CRYPTOLINGUIST. As the work is often slow and painstaking, requiring the gathering of tiny acorns one at a time, it is essential that the CRYPTOLINGUIST enjoy certain considerations. These we assign the appropriate acronym: SOS.

1. SILENCE: The intensity and concentration required for a superior CRYPTOLINGUIST to accomplish often arduous tasks which includes sometimes extensive degarbling, cross-checking, and memorization, demands an atmosphere conducive to such endeavors. The tantamount among these is silence. Unpublished medical research has proven that each time the loudspeaker announces another esoteric meeting, over 2000 braincells in the average CRYPTOLINGUIST explode; and each time the CRYPTO-LINGUIST deep in thought is jarred by a ringing telephone, his or her remaining nerve cells are decimated. With all this documented medical knowledge and the piles of brain cells and nerve endings swept from the carpets each evening, the powers that be still haven't gotten this message.

(b)(3)-P.L. 86-36

2. OBJECTIVE: The on-again, off-again nature of staffer and management decisions vis-a-vis the operational target of a CRYPTOLINGUIST is even more frustrating than the phone and the intrusive loudspeaker. Somebody should decide what we should direct our efforts toward and stick to it. A good CRYPTOLINGUIST like a good German Shepherd needs to be given challenging objectives and an occasional pat on the head.

3. SUPPORT: There are many challenging tasks available to the CRYPTOLINGUIST, some which go to State-of-the-art, and others which represent maintaining continuity on various projects. All such efforts affect the mental health and job comfort of the CRYPTOLINGUIST. Often, instead of fighting to see that CRYPTOLINGUISTS are provided with such work, management is more concerned about political ramifications, inter-office harmony, ethics seminars, etc. SIGINT has become an afterthought if that. Based on this assessment, we consider that this is a very bad time in our history to consider making a career move to that of CRYPTOLINGUIST. The CRYPTOLINGUIST may be an intelligent and capable animal, but it is also on the endangered species list.

So the three acronyms sum up what it means to be a CRYPTOLINGUIST today: MID-LIFE SOS.

****
//////////

7. COMMUNITY SERVICE

(U) a. From [redacted] come two interesting items about the ACA, who and what it is, and one of its services.

The American Cryptogram Association (ACA)

It's 3 p.m. on Saturday. The rain will continue till evening and you don't want to go out. You need a mental stimulator to keep from napping, so what to do???

If you had joined the ACA that would be NO PROBLEM! You would take the bimonthly ACA journal, The Cryptogram, off the shelf, grab some graph paper and pencils, and start having fun. Some of the entries in the table of contents from a recent issue give you an idea of what's offered: Early Forms Porta Table, Solving the Magic Square, Bring Home the Baconian, Computer Column, Cipher Exchange, Cryptarithms, and many more. The Cryptogram is made up of ciphers in systems that can certainly tickle your brain cells!! (b)(3)-P.L. 86-36

The ACA was started in the 1920s to further the enjoyment of cross-word puzzle solvers by offering cipher challenges created by ACA members. Systems are designed around classical pencil and paper methods. Ciphers include foreign languages; however, most are in English and can hide the wittiest and most entertaining prose. The ACA is a worldwide, non-profit organization which holds a yearly convention at which members get together and talk a unique ACA "cipher-speak" to their hearts' content.

Included in The Cryptogram are book reviews, methods-of-solution articles, unique cipher finds, occasional unsolved historical ciphers, answers to prior issue challenges, news about the members and more. The association itself is friendly; many members have been lifelong acquaintances thanks to the hobby of cryptograph promoted by the ACA.

For membership information, write to:

American Cryptogram Association
Treasurer
P. O. Box 198
Vernon Hills, IL 60061-0198

I know that there are ACA members out there! Maybe you would like to use this newsletter to let other people know about your experiences with cryptography as a hobby and/or your involvement in the ACA. We hope to hear from you.

[redacted]

(b)(3)-P.L. 86-36

[redacted]

American Cryptogram Association (ACA) Bulletin Board Service (BBS)

With your modem humming and your other favorite computer bulletin board busy, where do you go for some telecomputing fun?

(b) (6)

Have you dialed into Columbia, MD via [redacted] yet? There is your answer to an otherwise boring wait for a bulletin board to play on. When you get in, you will see that you have reached the "DECODE" BBS run by Mr. Dan Veeneman, who arrived last year from the Chicago area. Dan started this BBS there as the official BBS for the American Cryptogram Association.

This board caters to the international membership of the ACA, a group of cipher solvers with a history back to the early 1920s. Non-ACA members are allowed to use the board (in fact they are encouraged) as an opportunity to meet the ACA or at least find interesting downloads for cryptography buffs. Besides carrying information of use and interest to hobby cryptanalysts, the free BBS also offers email posting, USENET news, huge wordlist files, and in the future, access to Internet.

The ACA Computer Supplement, offering a wide variety of programming language source code and software development articles, is one of the most popular downloads from the board. All the cipher challenges from the bi-monthly journal of the ACA, The Cryptogram, may also be accessed from this BBS.

To contact Dan in Columbia, send correspondence to:

American Cryptogram Association
P.O. Box 2442
Columbia, MD 21045-2442

Facsimile may also be sent via the phone number provided above.

b. (U) Apples Needed Apples for the Students

On September 18th, 1994 Giant Food began its `Apples for the Students' program again. This program allows area schools to redeem cash register receipts for computer equipment. For the last several years, CMI has collected receipts and donated them to a needy school. Last year's choice was the Ruth Parker Eason School in Anne Arundel County. It is a special education school where many of the students are multiply handicapped. With our help they were able to purchase a new Macintosh computer with a CD Rom and a printer.

This year, CMI will again collect receipts. Suggestions are being accepted for a recipient school. (Last year's school will also be considered again.) Please send the bottom portions of any receipts that you would like to donate to [redacted] HQ. Suggestions for needy schools may be sent to [redacted] HQ, [redacted] Thank you.

(b)(3)-P.L. 86-36

c. Cryptologic Almanac

~~(S-CCO)~~ The Center for Cryptologic History (E324) regularly

[redacted]

publishes a feature known as "Cryptologic Almanac." These items relate an important or just plain interesting event in the history of cryptology. An almanac story may be classified, such as recent discussions of Project BOURBON and the "myth" of Black Friday, or it may tell an unclassified tale such as contrasting portraits of NSA deputy directors or the uses of codes and ciphers during the Civil War. Future articles will deal with American efforts to build its own Bombe during World War II, [redacted]

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

Here is a recent sample:

The Passing of Solomon Kullback

(U) Friday, 5 August, marked the passing of one of America's greatest cryptanalysts. Solomon Kullback, part of a team that broke Japan's first machine ciphers in the mid-1930s, died at Holy Cross Hospital in Silver Spring.

(U) Kullback was born in Brooklyn in 1907. He was a brilliant mathematics student and obtained a B.S. in math from City College of New York and an M.A. (also in math) from Columbia. Kullback was hired by William Friedman, head of the Army's cryptologic organization, in 1930. He entered on duty almost simultaneously with Frank Rowlett and Abraham Sinkov, and all became pioneers, with William Friedman, in America's cryptologic business. When the Japanese introduced their first diplomatic machine cipher in 1935, this team broke it almost immediately. When its successor system, Purple, was introduced in 1938, they also broke that (after two years), thus enabling America to read Japan's diplomatic ciphers throughout the war. Paradoxically, though, Kullback moved on to head the Army's effort against Germany, not Japan, during the war years.

(U) Kullback earned his Ph.D. in statistics from George Washington University in 1934, and taught classes there for years. After the war, he became director of research and development for the Army Security Agency. When the Armed Forces Security Agency was formed, he became its technical director of R & D,and in 1957 was named assistant director of R & D for NSA. After his retirement from government service in 1962, Kullback became head of George Washington University's department of statistics. He authored three books and many journal articles on mathematics and statistics, and he was widely respected in those fields. When Kullback retired from George Washington in 1972, he was awarded the title of professor emeritus.

(U) Of the original four members of the team who broke the Japanese ciphers, two survive. Frank Rowlett lives in Florida, and Abe Sinkov is in Arizona. William Friedman died in 1969.

[Thomas R. Johnson, Center for Cryptologic History, [redacted]

(FOUO) Barry Carleen, E324, is the POC for Cryptologic Almanac items and he posts articles like the one above to the Electronic Subscription Service (ESS) and to ENLIGHTEN.

(b)(3)-P.L. 86-36

(FOUO) To access the Cryptologic Almanac, simply add topic 1364 (Center for Cryptologic History) to your ESS distribution, or look on ENLIGHTEN under the topic "pubs.history". [If you don't know how to

[redacted]

subscribe to ESS or how to access ENLIGHTEN topics, please contact [redacted] who will e-mail you very explicit instructions.]

d. (U) National Cryptologic Museum News - from Jack Ingram, Curator

Have you ever heard of the Hebern Electric Code? It was the first American cipher machine to embody the wired rotor technique. Edward Hebern invented the rotor and the the first electromechanical machine in 1918. The machine now on permanent display at the Cryptologic Museum is beautifully made of solid brass, and features a single rotor and keyboard.

Come and see this, and other fascinating items on display at the Museum which is now open on Saturdays hours, from 1000-1400.

e. (U) Math Speakers' Bureau

NSA's Mathematics Speakers Bureau is looking to expand its current course offerings on science related topics and needs volunteers to develop some talks. You don't have to have any particular type of background to help out--and the field of possible topics is a wide one (astronomy, physics, chemistry, etc). If you're interested, please contact [redacted] at [redacted] Thanks.

(b) (3)-P.L. 86-36

//

8. AN OPEN LETTER TO THE CA COMMUNITY

(U) Shrinking resources and a changing world are forcing all of us to rethink and reevaluate our jobs. Open and honest expression of opinions are critical for building a healthy understanding of where we are and where we need to be. Unfortunately, in free-flowing debate on sensitive issues misspeaking and misunderstanding can occur all too easily. At a cryptologic futures committee meeting such a miscommunication occurred. The publication of the CA conference proceedings brought the miscommunication to light and prompted us to confront our feelings about the math/CA divide. You may recall that in her impassioned, if somewhat reckless, speech [redacted] implied that [redacted] was not a friend of cryptanalysts. This struck [redacted] as a bit unfair, as he has spent much of his career not only befriending cryptanalysts but being one! He has on many occasions experienced and profited from the worthwhile and productive efforts of graduates of the CA intern program from all decades. We tried to understand the dynamics of a situation that seems to place us on different teams though we seek the same goal.

(b) (3)-P.L. 86-36

(U) The cryptanalyst's feeling that he is in competition with the mathematician is both reality and projection. We define ourselves not only by what we think we are, but by what we believe we are not. Women and men perform many of the same functions, yet they have certain specializations that are crucial to the survival of our species. What would we say if told that we could only have one or the other? Though cryptanalysts and mathematicians at work are often indistinguishable from each other, each discipline has different emphases and preferred modes of thinking. When a situation comes along that demands these specialized skills, we are fortunate still to have both types of people at this Agency. How do men and women manage to co-exist? Recognition

of mutual need. This can work for us too.

(U) The conference tried to focus on what cryptanalysis is and identified a wide range of problems for which the cryptanalyst is needed. That vision of the cryptanalyst's future needs to be well-understood within the field and then effectively communicated to the other disciplines with which it is entwined. As the understanding of our mutual need is built, mutual respect will grow.

[redacted]

//

9. LITERARY TIDBITS

a. (U) "Decrypting" ISBNs [redacted]

(b)(3)-P.L. 86-36

The International Standard Book Number, or ISBN, is a 10-character string which uniquely identifies a book. The ISBN was adopted by American book publishers in 1967 and by the International Standards Organization in 1969 in order to facilitate the process of ordering and inventorying books by computer.

The first nine characters are always digits, the tenth can be any of the digits 0-9 or the character X, which represents the number 10. These ten characters can be separated into four fields. The first three are of variable length while the fourth consists of a single character.

The leftmost field is called the Group Identifier. It identifies a group of publishers. For example, a `0' or `1' means that the book was published in an English-speaking country, while a `2' means that it was published in a French-speaking country, and a `3' means that it was published in a German-speaking country.

The second and third fields, called the Publisher Identifier and Title Identifier respectively, are used to identify a specific publisher within the group, and a specific book title put out by that publisher. A prolific publisher will have a short Publisher Identifier field and a long Title Identifier field.

The final field is a check character. It is selected so that when one performs a dot product between the ISBN and the vector (X=10,9,8,7,6,5,4,3,2,1,0), the answer is equal to 0 modulo 11.

For example, consider the ISBN 052142707X.

```
 X  9  8  7  6  5  4  3  2  1
 0  5  2  1  4  2  7  0  7  X
 ___________________________
00+45+16+07+24+10+28+00+14+ X  = 154 = 0 (mod 11).
```

(b)(1)
(b)(3)-P.L. 86-36

b. ~~(FOUO)~~ Crypt History in the First Person

~~(TSC)~~ Prior to his retirement, former Chief Z, Mr. Harry Hoover authored a paper, [redacted] which was recently distributed to each Z branch. If you haven't seen the paper yet and would like to, you may contact:

[redacted]

[redacted] or by e-mail ([redacted]. The paper is available in either hard copy or soft copy.

.....

//

10. ACTION LINE

(U) QUESTION: What was the selection process for attendees for the 1994 C/A Conference? How can someone increase his/her chances of attending the next conference?

ANSWER: (Provided by [redacted] Chairman of the CA Career Panel)

The Career Panel's January conferences have served to address issues which are felt to be of importance to cryptanalysts. The 1993 conference dealt primarily with management issues, in light of the reorganization. The 1994 conference had two related thrusts: the new technologies and the direction in which cryptanalysis is moving. Of course, the attendees feel free to debate many other issues as well.

Attendees at the conferences are selected with the theme of the conference in mind. Senior Z management is usually invited regardless of the topic. The Panel tries to select people who will contribute to the discussion sessions and who can be expected to continue the discourse with those who could not attend. An effort is made to spread attendance over Offices, and to invite a fair number of junior cryptanalysts. Those who are not certified in cryptanalysis are rarely invited.

The 1993 conference included about [redacted] analysts; in 1994 the list swelled to [redacted] and we prefer the greater number if the theme permits. The theme has not yet been chosen for 1995. One possibility is the difficulty we in Z face in convincing qualified people to assume management positions. Has the management-technical pendulum swung too far? What can be done to make first-line management positions more attractive? Suggestions for other topics would be appreciated, but the decision needs to be made very soon, so do not delay proposing topics of community-wide interest. Call the Executive, [redacted] with your suggestion.

The best ways for a cryptanalyst to increase his/her chances of being selected for the annual cryptanalysis conference are to express his/her interest in attending by participating in cryptanalysis activities throughout the community, performing excellent work in the operational arena, and contacting the C/A Career Panel, H111, Ops #2B, [redacted].

Interested parties may also be sure that their names will appear on a consideration list by sending email to either the Executive of the C/A Career Panel, [redacted] or her assistant, [redacted]

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

//

11. (U) PUZZLES

a. Solution to "Equations"

1 = Flew Over the Cuckoo's Nest

```
   1 = Wheel on a Unicycle
   3 = Blind Mice (See How They Run)
   3 = Sheets to the Wind
   4 = Faces of Presidents on Mount Rushmore
   4 = Quarts in a Gallon
   4 = Families of Musical Instruments
   6 = Legs on an Insect
   6 = Pockets in a Pool Table
   6 = Wives of Henry the Eighth
   7 = Stars in the Big Dipper
   7 = Voyages of Sinbad
   7 = Wonders of the Ancient World
   8 = Sides on a Stop Sign
   8 = Notes in an Octave
   9 = Planets in the Solar System
  10 = Little Indians
  11 = Players on a Football Team
  12 = Angry Men
  12 = Labors of Hercules
  12 = Signs of the Zodiac
  13 = Stripes on the American Flag
  14 = Days in a Fortnight
  16 = Ounces in a Pound/Pint
  18 = Holes on a Golf Course
  18 = Wheels on a Tractor-Trailer
  24 = Blackbirds Baked in a Pie
  24 = Hours in a Day
  26 = Letters in the Alphabet
  29 = Days in February in a Leap Year
  31 = Flavors of Ice Cream at Baskin-Robbins
  32 = Degrees Fahrenheit at which Water Freezes
  40 = Days and Nights of the Great Flood
  40 = Channels on a CB Radio
  54 = Cards in a Deck (with the Jokers)
  57 = Heinz Varieties
  64 = Squares on a Checker/Chess Board
  66 = Books of the Bible (King James Version)
  76 = Trombones that Led the Big Parade
  80 = Days to Go Around the World
  88 = Piano Keys
  90 = Degrees in a Right Angle
 101 = Dalmatians
 200 = Dollars for Passing Go in Monopoly
 206 = Bones in the Human Body
1000 = Words that a Picture is Worth
1001 = Arabian Nights
1215 = Year the Magna Carta was Signed
1760 = Yards in a Mile
20000 = Leagues Under the Sea
```

****

b. ARBOR DAY by [redacted] (b)(3)-P.L. 86-36

I was curious about the scientific names of some of the trees found in the Ft. Meade area (and maybe even a few that aren't), so I went and looked them up. However, I think that the author of the book I consulted was more cryptographer than botanist, because the names I found there looked a little suspicious. They turned out to be nothing more than encrypted versions of the trees' common names (some of which

are two-word names). Half of each 'scientific' name was a uniliteral monoalphabetic substitution of the common name, and the other half a Playfair substitution of the same name, although the author was pretty sloppy about the order; either substitution could come first. He was kind enough, however, to use the same plain and cipher alphabets and the same square for all of the trees. See if you can decipher the trees and recover the keywords on which the substitutions are based. (A different keyword was used for each method.) If you can, mail the solution to [redacted] and you will receive the coveted honor of having your name printed in the next issue.

(b)(3)-P.L. 86-36

1. Mzarqimc cbfhkqwi	9. Gmqhmbvfuk beapkdrork
2. Swzuqjfw owhpmuaw	10. Kdfive mbkddn
3. Biblbiriib gwggwydwg	11. Dkxmkxwd iftdcfit
4. Gaqpbmersi xqlzjwgyfd	12. Bsdoniotsk glzwdswvjk
5. Awqawa cbaubc	13. Mbkghulh kdfevpbp
6. Xqzcqqx gazowuag	14. Xusqurpsyc ajlkgvdlmk
7. Simpmiag fdqucqqx	15. Owgmdovk swbqzwun
8. Hkwi rcmc	16. Sljakddn oluxfive

****
//////////
****

12. EDITORIAL CORNER

If you have a relatively short technical treatise, or anything you would like to have considered for inclusion in future issues, please submit it to any member of the editorial board or any of our office POCs.

PLEASE paragraph classify each item submitted, and USE ASCII FORMAT!

A reminder that anonymity may be requested for Action Line items - in fact, you may mail them in hardcopy form to any member of the editorial board or any of our office representatives.

We would very much like this newsletter to represent a broad cross-section of the CA community - we need some more volunteers to help us, however. Perhaps you would like to work on one of the topics in this issue, or perhaps there is another topic which you think should be included in future issues. Either way, we would like your input, and help, so give one of us a call. The more people who divide up the work, the less burden on any one person.

##########
NOTE: We MUST receive any submissions for the November issue by 21 Oct.
##########

EDITORIAL BOARD

[redacted]

(b)(3)-P.L. 86-36

[redacted]

Jack Ingram, Cryptologic History Museum
[redacted] NCS

OFFICE Reps

[redacted]

(b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

[redacted]

(b)(3)-P.L. 86-36

[redacted]

TOP SECRET//COMINT

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:16
(U)PE EXTERNAL PAGE

[redacted] (b)(3)-P.L. 86-36

****
* TALES OF THE KRYPT *
****

November 1994

##########
//////////

(U) TABLE OF CONTENTS:

1. Perspectives in CA - [redacted]

2. KRYPTOS Society

3. Calendar of Events

4. Word from the CACP
   a. Professionalizations
   b. Panel Changes
   c. Panel Actions
   d. Biographical Portrait
   e. 1995 CA Conference Update
   f. BANCC Notice

5. Technical Health
   a. Cryptanalyst to the Hinterlands
   b. PUPs (Pop-Up-Prompt Tutorials)

6. Community Service
   a. Apples for the Students
   b. NSA's Attic
   c. Russian Visitors to the Cryptologic Museum
   d. PURPLE Analog on Display at Cryptologic Museum
   e. Cryptologic Literature Awards

7. Action Line

8. Puzzles and Problems

9. Literary Tidbit

10. Editorial Corner

##########
//////////

1. (~~FOUO~~) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice, and we alternate between Seniors from within Z and Seniors outside Z. This month we are pleased to print the thoughts of [redacted]

~~(C)~~ Hi, I'm [redacted] currently chief of [redacted]

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted] (b)(3)-P.L. 86-36

[redacted]

[redacted] The first eight years of my Agency career were spent on a variety of SIGINT and COMSEC analytic problems as a member of the P1 program (now CMP), in [redacted] and as an integree at GCHQ (still GCHQ). (b)(3)-P.L. 86-36

(S) Cryptography has changed in significant ways since the seventies, when I was last working in INFOSEC. Since it is still true that the current developments in the INFOSEC business are often experienced a few years later in the SIGINT business, I'd like to share them with you.

(C) Cryptography is expected to provide many more security services. Here is a quote from a recent Advanced Research Programs Agency (ARPA, formerly DARPA) solicitation for unclassified research proposals to supply advanced security technologies for the National Information Infrastructure (NII). "These services could include authentication, authorization, confidentiality, access control, auditing, audit analysis, integrity, key management, and multiparty key escrow." Cryptography, either conventional or public, is the basis for all of these services except those dealing with audit.

[redacted] (b)(1) (b)(3)-P.L. 86-36

(S) Cryptography is no longer a discipline almost exclusively dominated by a few national agencies. Public knowledge and sophistication in all aspects of cryptography and its uses have increased considerably.

[redacted] Get a copy of Bruce Schneier's book, "Applied Cryptography", if you haven't already, and spend some time reading it. It is a very readable compendium of the public knowledge of cryptography, the available algorithms, and the potential applications. Of course, as good as this knowledge is, there is still plenty of room for mistakes in converting theory to practice. [redacted]

(S) What is the import of all this to cryptanalysis? There is a

[redacted] (b)(3)-P.L. 86-36

growing realization that the United States national interests are at serious risk because we rely so heavily on security vulnerable network communications and computers for running our economy and our defenses. It is that feeling that has prompted the ARPA solicitation from which I quoted above and is pushing forward the public knowledge of cryptography and its uses. However, if the United States buttons up its communications networks there is the very real danger that everyone else will also, either by following our example or to preserve interoperability with our networks. There is enormous pressure from U.S. hardware and software manufacturers to allow the export of the same security products abroad as they produce for the domestic market. The end result could be a considerable loss of access to communications and data, both plain text and enciphered, that produce SIGINT. Key escrow as embodied in CLIPPER/CAPSTONE is an example of an approach to solving this problem.

(S) The battles over issues like key escrow and export control are being very strongly fought by the leadership of the Agency and there is every hope that they will continue to be successful, but even if they fail there is still a bright future for cryptanalysis. In my view the most exciting feature of cryptanalysis is its concentration on solving the problem regardless of the technique that has to be used. How often have we seen a cryptanalytic problem seem unsolvable by conventional attack, and then seen it fall by the clever application of some "sneaky" trick. It is that kind of attack mentality that promises to be the greatest virtue of future cryptanalysis. In the future the front door is likely to be made of hardened steel with a strong cryptographic lock, but it is also likely that a back window will be left unlocked. The tight integration of cryptography in complex uncontrolled systems, which is such a challenge to INFOSEC, can be a great benefit to cryptanalysts, if we are willing to take on the challenge. It may in some cases mean we are fishing with spear guns instead of with trawlers, but we can hope to land more valuable, though fewer, fish.

(U) Willingness to change and willingness to accept new challenges has always been a hallmark of the cryptanalytic effort at the Agency. How to get started seems to be the hard question right now. There are no established courses or text materials. I don't believe it is even clear what subjects the new courses should address in depth. It will take time and experience to develop the appropriate training. The history of cryptanalysis shows what a difficult process it has been to develop the tools and training which we accept as standard. After all Friedman's "Military Cryptanalysis" did not emerge full grown. Much of that material took many years to develop. If as a community we pool our resources, our knowledge, and most importantly our experiences solving the new problems, we can produce the training that we all need.

(C) In the meantime here are some areas in which to start. First any cryptanalyst who wants to work in this area should become familiar with the cryptographic principles which will supply all those services listed above. Conventional encipherment is only one feature. Signatures, hashing, and certificates are probably going to be as important or more so. To quote Rick Proto, "The cryptanalyst of the future may really be a forger" or at least that should be one of the available tricks. Secondly, the cryptanalyst needs to understand how cryptography is used in a modern system (analogous to the principle of understanding the properties of the underlying plain text). Most of us use [redacted] but do we know how it works and where the weak points are. How about PGP? These are e-mail systems. There will be a lot more cryptographic challenges and cryptanalytic opportunities in more

(b)(3)-P.L. 86-36

[redacted]

complex systems like [redacted] or network management as people try to bring security to them. A third area where some experience and knowledge would be useful is in network protocols. What are IP, ATM, and SONET?

(U) Thanks for reading this far. If you want more to read, one of my more notorious jobs was chairing a committee which last year looked at the future of cryptology. If you'd like a soft copy of the report, please send me an e-mail note at [redacted] and I'll send you a FrameMaker version.

(b)(3)-P.L. 86-36

****
//////////

2. (U) KRYPTOS

DON'T MISS THE NOVEMBER KRYPTOS TALK!

(U) In the January 1994 issue of WASHINGTONIAN magazine, an article by Ronald Jaffe detailed the work of U.S. Marshall Bill Bonk in the pursuit and capture of a fugitive wanted for murder. The article mentions the involvement of "decoding specialists". Marshall Bonk and the "decoding specialists" will give a presentation of this fascinating case at the November meeting of the KRYPTOS Society which will be held on Tuesday, 22 November, in Friedman Auditorium, at 0900.

(U) If you have suggestions for future KRYPTOS talks, or if you would be willing to be a speaker, please contact [redacted] D/CH. Z3, who is the KRYPTOS Program Chair. He can be reached via e-mail, [redacted] or by phone at [redacted]

****
//////////

3. ~~(FOUO)~~ CALENDAR OF EVENTS

Nov 3	CMI TAlk (0930 Friedman) "SCAMP 1994" [redacted]
Nov 4	KRYPTOS Luncheon (1130, Officers' Club)
Nov 8-10	Data Demodulation Workshop (FanxII)
Nov 11-12	MD/DC/VA Section of the MAA Fall Meeting Western Md College
Nov 14-Dec 12	Health Benefits Open Season
Nov 21	PERSUMs - (9A135, 0930) Panel of Z Managers discusses the How's,Why's, When's and What's
Nov 22	KRYPTOS Talk - (0900, Friedman)
Dec 1	CMI Talk [redacted] (0930, Friedman)

(b)(3)-P.L. 86-36

PLAN AHEAD:

[redacted]

	Jan 18, 1995	BANCC (see CACP News)
	Jan 24-25, 1995	1995 Cryptanalysis Conference (SRC)
	March 27-31, 1995	CARD (GCHQ)
	May 23-25, 1995	CA PQE
**	Jun 5 - 9, 1995	CA-305 (** NOTE - this is a change.)

//

4. (U) CACP News

a. CRYPTANALYSIS PROFESSIONALIZATIONS:

[redacted] (b)(3)-P.L. 86-36

b. Panel Changes

[redacted] Z32 (replaces [redacted] PCSing to CCR-LJ)

c. Panel Actions

The CACP approved new guidelines for the Technical Paper and the Computer Program Requirements for CA certification. They go into effect on 1 November 1994. Copies may be obtained from the CACP office.

PLEASE NOTE: CA-305 dates have changed. It will now be held from 5 to 9 June 1995.

d. ~~(C)~~ BIOGRAPHICAL PORTRAIT

The CA Panel has said farewell to their first military advisor, [redacted] The former [redacted] served on the CA Panel from March 1994 to July 1994 as a liaison between military CA aspirants and the CA Panel. (b)(3)-P.L. 86-36 (b)(6)

[redacted]

[redacted] While serving on the Panel, [redacted] most enjoyed the overview of the CA community and its issues. He believes the idea of having a military representative on the Panel serves a dual interest to the CA community and to the technical health of many participating military members.

[redacted] (b)(3)-P.L. 86-36

[redacted]

[redacted]

e. (U) CA Conference Update

The CACP has decided on "Technical Health in the CA Community" as the theme for the 1995 CA Conference. The Panel is still in the early stages of planning the conference but hopes to identify and design specific technical development offerings (courses, working aids, seminar series, etc.) during the conference. The Panel is open to suggestions for this theme, and asks that you forward them to Donna, Joella, or any Panel member. Also, the Panel is accepting self-nomination requests for attendance at the conference. Names should be forwarded to [redacted] (b)(3)-P.L. 86-36

f. (U) BANCC

There will be a Breakfast Affair for Newly-Certified Cryptanalysts (BANCC) in the Canine Suite on 18 January 1995.

//

5. TECHNICAL HEALTH

a. (U) CRYPTANALYST TO THE HINTERLANDS by [redacted] Z433

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(S-CCO) After several years away from cryptanalysis, I decided to return to that field in 1992. Since I had enjoyed working as a

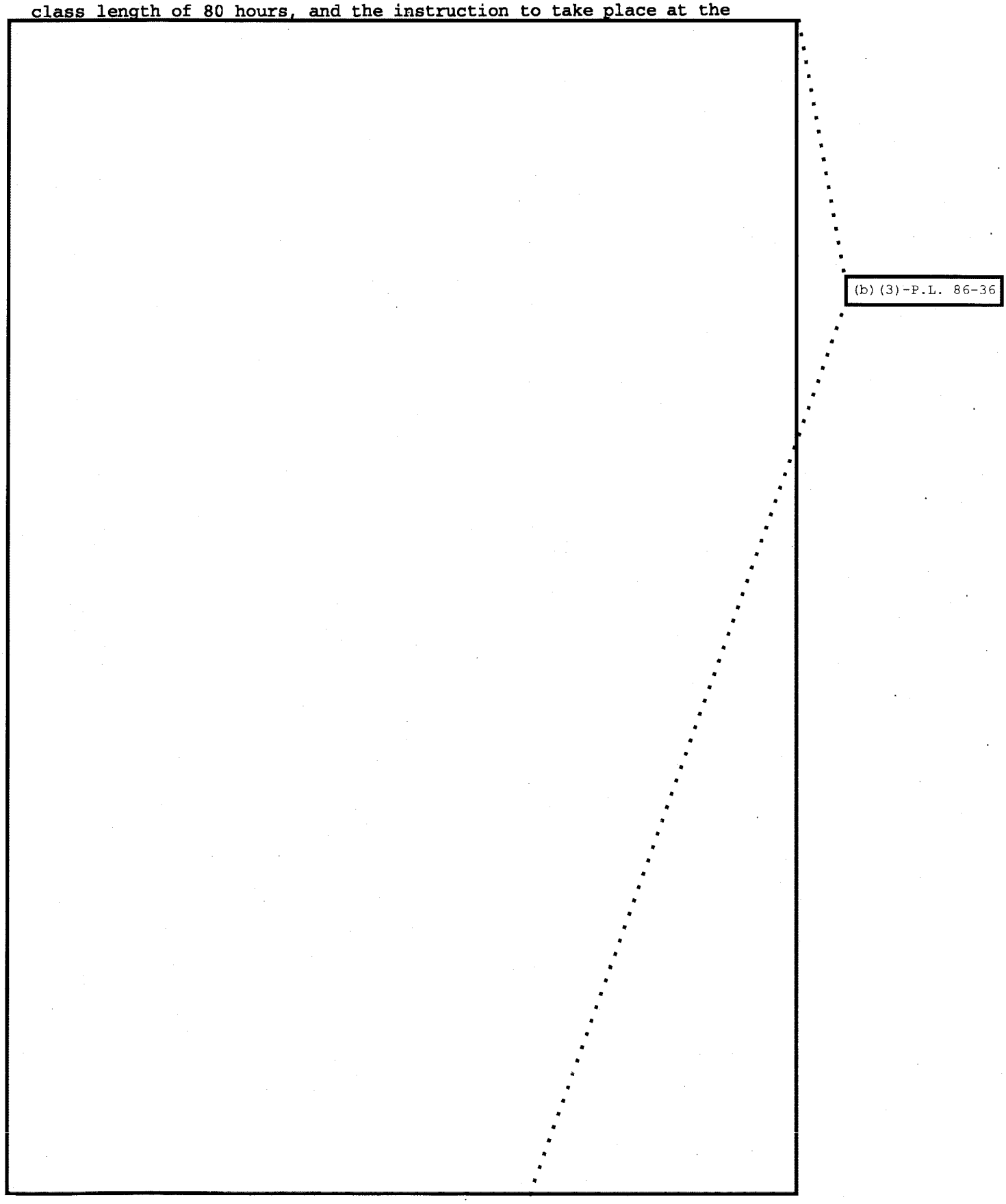
[redacted]

(FOUO) Around the same time, E4 announced the SLANG and SPICE programs for external language training. E4 told me that if I could find a place where [redacted] there might be a chance that I could go, if I applied and was accepted. I applied and somehow got accepted. Thus began a long dialog with administrators of the [redacted] the language department there, and

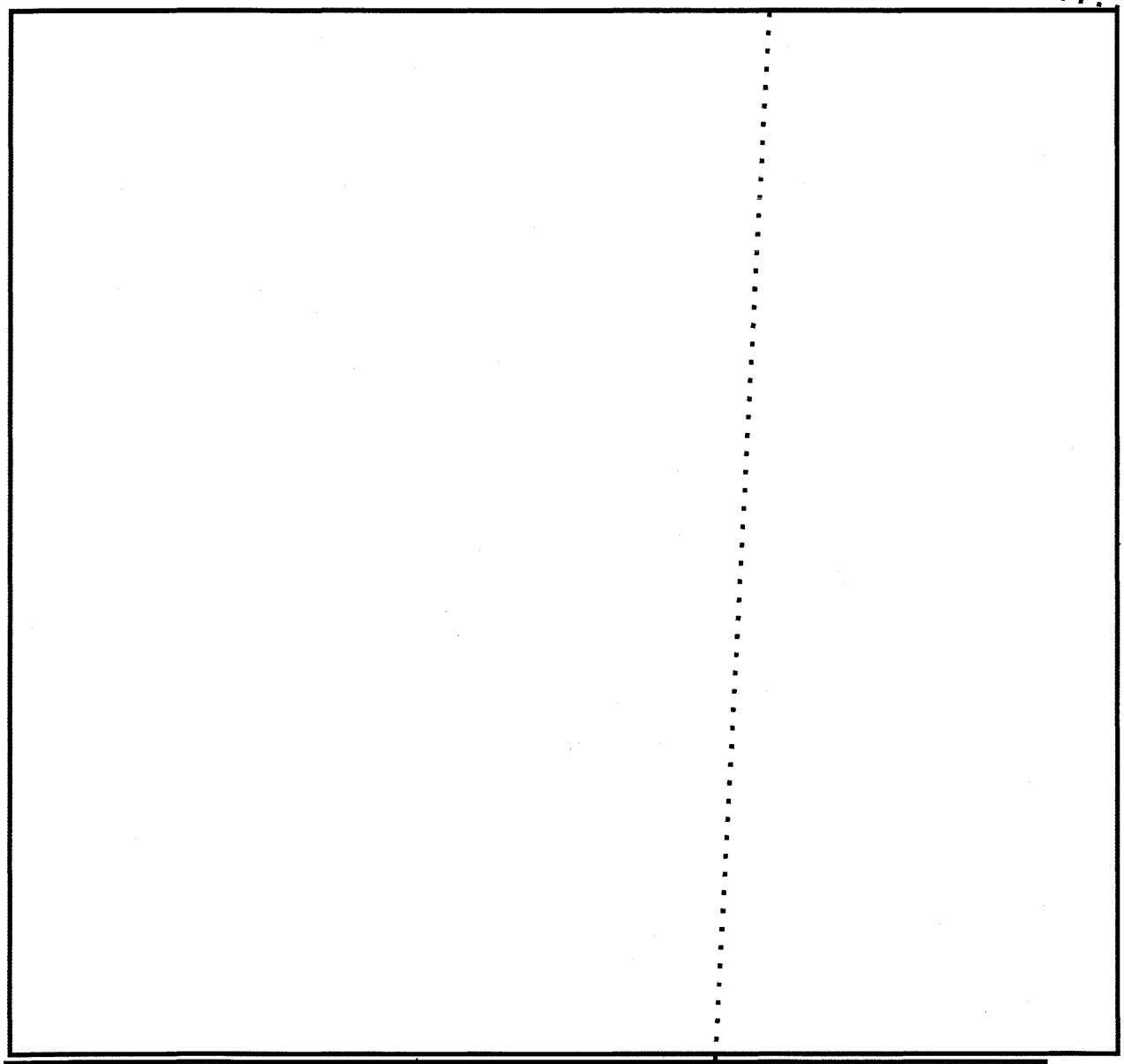
(b)(3)-P.L. 86-36

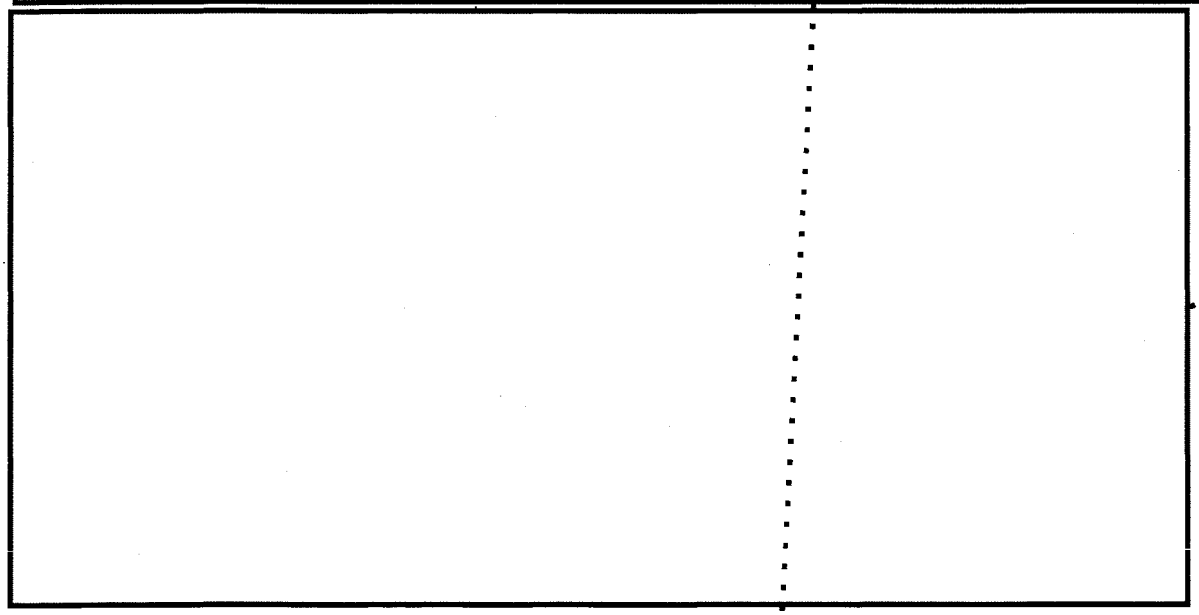
[redacted]

with the future instructor to decide the dates, place, and length of the class. The month of June 1994 was chosen as the most convenient, a class length of 80 hours, and the instruction to take place at the



(b) (3)-P.L. 86-36





(b) (1)
(b) (3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

b. (U) A New Approach to On-line Computer Tutorials

(U) What is a PUP?
a. a small dog
b. an on-line computer tutorial
c. a kind of tent
d. all of the above

(U) Answer: d. all of the above. What, you didn't know about the on-line computer tutorial? PUPs are Pop-Up-Prompt Tutorials and the first one was written for FrameMaker 2 about two years ago. Since then 20 PUPs for a wide variety of software products have been designed and are in various stages of development. These include two of special interest to Z users, the DPP PUP and the ZAP PUP.

(b)(3)-P.L. 86-36

(U) These tutorials are designed by groups of users, with editorial and leadership guidance by the Computer Based Tutorial for Users Council (CBTUC). The CBTUC is a group of 15 volunteers from many disciplines (cryptanalysis, language, reporting, computer science) and many groups (A, B, J, Z) in the Agency. The chairperson is the PUP Director. Currently, [redacted] is the PUP Director.

(U) What makes these tutorials different than the ones which come with the software? PUP Tutorials are designed to run alongside the software which is being learned so that the learning process happens as the software is used. The skills which are learned follow a logical progression of tasks from easiest to most complex, or from start to finish of a particular project. For example, the FrameMaker 4 PUP takes the learner from creating a blank document to adding text to adding titles to adding page classifications, with minor formatting steps in between.

(U) Why should I use the PUP tutorial rather than going to a class?

You shouldn't, because the class is a very useful experience, and covers many things which are not covered in the PUP tutorial. But, if you are having difficulty getting into the class, if you want a reference after you get out of class, if there is no class offered, or if you prefer to work at your desk at your own pace, you might want to use the PUP tutorial.

(U) Tired of answering the same questions over and over from those around you new to the software? If you would like information on having a PUP tutorial developed, would like to know what other PUPs are available, would like to see a demonstration, or would like to be a PUP tutorial writer, contact [redacted]

****
//////////

6. COMMUNITY SERVICE

a. (U) Apples Needed - Apples for the Students

On September 18th 1994 Giant Food began its `Apples for the Students' program again. This program allows area schools to redeem cash register receipts for computer equipment. For the last several years, CMI has collected receipts and donated them to a needy school. Last year's choice was the Ruth Parker Eason School in Anne Arundel County. It is a special education school where many of the students are multiply handicapped. With our help they were able to purchase a new Macintosh computer with a CD Rom and a printer.

This year, CMI will again collect receipts. Suggestions are being accepted for a recipient school. (Last year's school will also be considered again.) Please send the bottom portions of any receipts that you would like to donate to [redacted] HQ. (She is also collecting SAFEWAY receipts for a similar program.) Suggestions for needy schools may be sent to [redacted] HQ, [redacted]. Thank you.

(b)(3)-P.L. 86-36

****

b. ~~(C)~~ NSA'S ATTIC (#10-94)

I. INTRODUCTION

(U) These notes were prepared by the NSA/CSS Archives to acquaint customers with the type of cryptologic material held by the Archives and how to access it - perhaps for research purposes or to support current operations. Material is available on a need-to-know basis and researchers must be properly cleared before gaining access to the records. For further information, phone [redacted] or send an E Mail to [redacted]

II. ACCESSIONS

1. Early History of the United States Air Force Security Service (Accession 46593) (U)

(U) This accession covers the history of the United States Air Force Security Service (USAFSS) from 20 October 1948 to 31 December 1949. Chapter headings include the establishment and

[redacted]

development of the USAFSS, the mission of the USAFSS in the Air Force, the transfer of units and responsibilities from the Department of the Army to the Department of the Air Force, funding for the USAFSS, and the establishment of the USAFSS at Brooks Air Force Base in San Antonio, Texas. Additional topics include problems associated with the movement of personnel overseas, promotion policies, job assignments, training, and COMSEC (Communications Security) issues. The document is 170 pages in length and was written by Air Force Historical Technician T/Sgt Rupert P. Roberson.

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

[redacted]

3. The Sorge Spy Ring: A Case Study in International Espionage in the Far East. (Accession 45018) (U)

(U) For nine productive years a daring and skillful band of spies worked in Japan and China for their spiritual fatherland, Soviet Russia. Despite their vigorous activity and enormous successes they went unsuspected and undetected until 1941. Led by Dr. Richard Sorge, a German communist posing convincingly as a loyal Nazi, the ring of spies succeeded in keeping the Soviet Union fully informed on Japanese military and industrial capabilities and intentions from 1933-1941. During this period the Red Army always knew the status of current Japanese war plans and could make their own plans and dispositions accordingly. This accession (with photographs) details how Sorge organized his spy ring, the ciphers and communications procedures his spy ring used, and how he was eventually discovered and imprisoned.

III. NOTES

ARCHIVAL EXHIBITS (U)

a. (U) "Pearl Harbor to Midway" - currently showing in the National Cryptologic Museum.

b. (U) "The Shootdown of Admiral Yamamoto" - on display at the NSA/CSS Archives.

c. (U) The "Capture of the German U-Boat 505" - on display at

(b)(3)-P.L. 86-36

[redacted]

the United States Naval Academy in Annapolis.

d. (U) "Deception at D-Day" - exhibit is currently being shown in the Special Collection Library at the National Defense University at Ft. Lesley J. McNair in Washington D.C. until 20 November.

e. (U) "Native American Code Talkers WW I and WW II" - a copy is now on permanent display at the National Cryptologic Museum.

f. (U) "Peace in the Pacific" - this new exhibit is scheduled to be shown for the first time in September 1995.

---

c. (U) STORY CONFIRMED - The Russians Were Here!

(U) You may have heard something about Russians visiting the National Cryptologic Museum recently. The story is true.

(U) On Wednesday, 5 October, two Russian army officers in uniform visited the museum--the first Russians (we know of) to do so. The visitors were Lieutenant General Ivan Milkuan, chief of the Russian Army Personnel Department, and Colonel Alexander Nikinov, curator of the Russian Army Military Museum. Their visit to NSA was strictly unofficial--the Russians had come to the United States to participate in ceremonies marking the fiftieth anniversary of World War II, and stopped at the museum on their own time.

(U) These unexpected visitors toured the museum for a little over two hours and, among other things, were quite interested in our exhibit on the KGB Museum, which they had never had a chance to visit in Moscow.

(U) Of more enduring importance during this visit, the Russian officers presented the museum with a small fragment from the U-2 aircraft piloted by Francis Gary Powers, who was shot down over the Soviet Union in 1960. This fragment is now on exhibit in the museum. The curator has temporarily placed it in a spare case until a proper display can be prepared.

(U) Interested in having a look at the U-2 fragment? Drop by the museum and ask the staff to see it.

[David A. Hatch, Director, Center for Cryptologic History, [redacted]

---

d. (U) FULL CIRCLE: (b)(3)-P.L. 86-36
THE PURPLE ANALOG ON DISPLAY AT THE NATIONAL CRYPTOLOGIC MUSEUM

(U) The National Cryptologic Museum has just put on display in its main hall the PURPLE Analog--the early processor which was used by the Americans to decipher the high-level Japanese diplomatic cipher known to us as "PURPLE."

(U) This processor was designed in 1940 by a team of cryptanalysts led by Frank Rowlett. The team analyzed Japanese traffic and made enlightened assumptions about how the Japanese cipher machine worked; they decided telephone switching devices were a likely choice for the target

machine's components and used switches to construct an "analog" for machine decryption. After the war, the Americans found their assumptions had been absolutely correct--the Japanese had indeed constructed the original machine with telephone switches!

(U) The PURPLE Analog on display in the museum was identified some years ago by Mr. Rowlett as the unit which decrypted the Japanese Foreign Ministry's last message on the eve of Pearl Harbor. A British author who has written extensively on World War II called it the "holy relic," only partly in jest. In many ways he was right: the PURPLE Analog heralded a brave new era in cryptanalysis, and it is not too much to say that the cryptologic community's modern machine development stems from its successes.

(U) The PURPLE Analog is now displayed beside one of the few surviving fragments of an original PURPLE machine. Drop by and ask the museum staff for more on the background of the effort against PURPLE and what it meant to America's efforts, first to avert war and then to win it.

[David A. Hatch, Director, Center for Cryptologic History, [redacted]

e. ~~(TSSU)~~ CRYPTOLOGIC LITERATURE AWARD PRESENTED

The 1993 Cryptologic Literature Awards were presented on 6 October 1994 by the National Cryptologic School Commandant, [redacted] to three individuals whose papers were judged the most outstanding by the Cryptologic Literature Review Board.

First place went to Nora L. Mackebee, recently retired from Z Group, for her paper, [redacted]

[redacted], took Second place honors for his paper, "PURPLE DRAGON: The Origin and Development of the United States OPSEC Program". (b)(3)-P.L. 86-36

[redacted] was this year's Third place winner for her paper, "The Technological Implications of Emerging Space Programs in Southeast Asian Countries".

This year's winning papers were selected by the Cryptologic Literature Review Board from over a dozen submissions. ES6 readers may obtain copies of the winning papers through [redacted], Archives and Records Management, Mr. Robert Hanyok, [redacted].

Former NSA Director, VADM L. H. Frost, USN, established the Cryptologic Literature Award in 1962 as the highest award to recognize contributions to the body of cryptologic literature.

****
//////////

7. (U) ACTION LINE

(U) In the last year or so, many highly qualified aspirants for CA certification have had their certification papers rejected by the CA panel. In some cases, the rejection letters have included insulting remarks pertaining to the authors' understanding of the subject. Furthermore, a study of the requirements for the paper and the

[redacted]

evaluation criteria shows some disagreement. Some aspirants have been so disgusted by the unprofessional actions of the CA Panel that they have decided to become certified in other discplines!

(U) Why are the CA panel and the TPEB (Technical Paper Evaluation Board) treating these aspirants harshly and not applying a consistent and professional evaluation of papers submitted?

- ANONYMOUS

(U) Dear ANONYMOUS,

It is our opinion that even an anonymous assertion that the Technical Paper Evaluation Board is harsh, inconsistent, and unprofessional deserves a response.

The Boards which review submitted papers and programs are selected by the Panel from our community's most experienced and respected cryptanalysts, with attention paid to diversity, so that many points of view will be represented.

It is natural that differing views will be taken of the merits of a particular paper or a particular program. That is why we seek the counsel of a senior panel. Our panel changes regularly (we like to get fresh viewpoints and, fortunately, we have always received wonderful support from our senior analysts, who are willing to donate their time for the good of the career field), so it is quite possible that a marginal paper or program might be approved by one panel but disapproved by a different panel at another time.

The standard of professionalism we seek on the Paper Board is one which is difficult to quantify. Some of our aspirants have never before authored a technical paper; they should be advised by their supervisors to study some successful models (available, for instance, in the Z Technical Library), and our Executives are available to suggest papers which may suit an individual's reading preferences. We expect that less experienced authors will spend several hours in consultation with their senior analyst in preparation of a satisfactory paper.

Unfortunately, not every aspirant views the completion of a technical paper in as positive a way as we do. For many, it is a loathsome burden which must be borne. Indeed, there is hardly a cryptanalyst who would not prefer to be carrying out challenging and exciting new analysis instead of fighting frustrating battles with software which makes the publication of papers such a chore.

Some papers which are submitted show clearly the unwillingness of the author to provide the detail and the explanation which could be so instructive to others who are required to learn from the analyst's experiences. Papers which are submitted for certification are expected to have arisen naturally in the course of an analyst's labors; the supervisor is expected to be eager to see a correct and properly documented paper published. Instead, our seniors on the Board are often asked to review papers upon which which neither the author nor the supervisor has expended much energy.

The Board is understandably anxious to discourage such behavior. The Board has learned that, unless they speak clearly to the

weaknesses of certain papers, the papers, only slightly modified to rectify a few identified errors, will soon reappear, begging for approval. If the Board's criticism seems strongly worded, its motives must be understood. Their object is to foster pride in the literature cryptanalysts produce, and it seems clear that, judging for example from the excellence of the papers which have been winning prizes in the Cryptologic Literature Contest, they have been succeeding! If, on occasion, a board member has made comments that were too harsh, we apologize and we will try to avoid such remarks in the future.

A cursory review of the technical paper requirements and the evaluation criteria revealed no disagreements. In fact, the guidelines are currently being revised and improved, and should be released very shortly. As with the other concerns expressed in this letter, it is difficult to supply a more detailed response unless more specific information is presented. Individuals with questions or concerns regarding any of the certification criteria are encouraged to address them directly to the Cryptanalysis Career Panel or the appropriate Evaluation Board.

Cryptanalysis Career Panel
Technical Paper Evaluation Board

****
////////////

8. (U) PUZZLES AND PROBLEMS

a. (U) First of all, congratulations to [redacted] Z22, who was the first to let us know that she noticed the change in the Masthead, from "Tales of the Crypt" to "Tales of the Krypt". She earned a sundae!

b. ~~(TSC)~~ We will be combining the Problem of the Month and the Puzzles and Challenges into one category, and some months may have items for all three, while others may not. [redacted] and [redacted] will continue as the editors. (b)(3)-P.L. 86-36

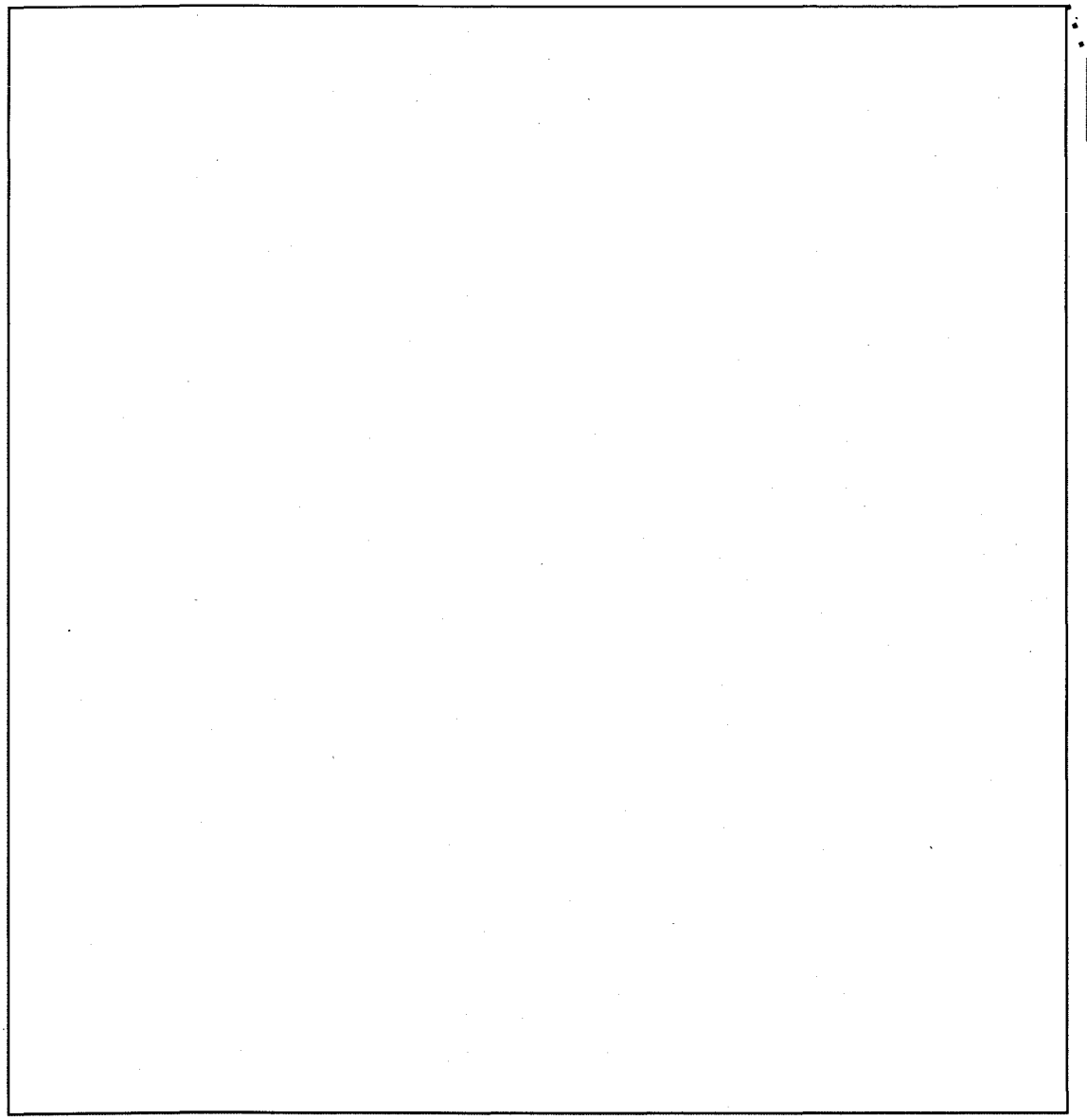
ANSWER TO SEPTEMBER PROBLEM OF THE MONTH

The September Problem of the Month consisted of [redacted] at Bad Aibling was the only person I heard from with a complete solution. [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

NOVEMBER PROBLEM OF THE MONTH

The Zendian ambassador to the U.S. has been using single transposition for 30 years, but he recently got a computer and jumped on the information superhighway. Unfortunately for us he subscribed to sci.crypt on the INTERNET and read that single transposition is insecure. As a result, he enciphered one last message stating that he was changing over to PGP. In his last transposition message he included some 256-bit PGP cryptovariables. It's a good thing I didn't make you break the transposition cipher with random hexadecimal values for plain text! The CV's are listed below.

What do we expect the next cryptovariable to be?

[++
6B5284F46BD62C2090633C3FCFFD0734DC67A3A52B26E2F4EF7E58451D735B7E
[++
69C8FD41470213F3EA6531B847F5AA73127593CABF6BC01F8118C5964D83F515

(b)(3)-P.L. 86-36

```
[++
D76E663E925FEA76B49715E12F1D3D62B8B4749FC2DF8FFA82E32298EDC3805C
[++
B445BEEB4EEBB0A9EDFAEABA8675BF02CD22442436834D85F4DD6E49FC33FB53
[++
024B07487AA7678C978CAE434EFD325153C005591957FCC0D607ABAA7CD365FA
[++
C0813F5615930D20B14E637C86B69550488EB63E6D5B9BAB2761D7BB6BA4C051
[++
EDE7681321AFA4633A4008652D9EE7FFAE8C56D3318F2946E9EBF47CCBA40A59
[++
8B7D81809CFB2B5634629CFF45B62A5E84BAE71864F3A8911BA501ED9BD44510
[++
9843899D8877A1F99DB42148CCFE5C6DC918680E0887178DBC8FFD0EDA347077
```

c. (U) Challenge from:

[redacted]

NSA Trivia question: Which Deputy Director has had his picture repainted to make it look more like the others. What was done?

d. (U) Solution to "Arbor Day"

1. White Oak
2. Magnolia
3. Sassafras
4. Douglas Fir
5. Baobab
6. Dogwood
7. Ironwood
8. Teak
9. Scotch Pine
10. Cherry
11. Red Cedar
12. Sugar Maple
13. Chestnut
14. Blue Spruce
15. Mahogany
16. Mulberry

(b)(3)-P.L. 86-36

The plain and cipher components of the uniliteral substitution are based on the key "Bristlecone Pine" with B-plain aligned with A-cipher. The Playfair square is based on the keyword "Sequoia", beginning in the center cell and spiralling clockwise outward.

Solvers

[redacted]

//

9. LITERARY TIDBIT

Edgar Allen Poe, Cryptologist

(U) At this time of year, we often think of Edgar Allen Poe, one of the more remarkable literary minds of antebellum America. His arabesque tales still have the power to make us shudder or grieve.

[redacted]

(U) Less well known is that Poe was an avid, if somewhat limited, cryptologist. In one of his lectures, William F. Friedman wrote, "[f]or his day he was certainly the best informed person in this country on cryptologic matters outside of the regular employees of government departments interested in the subject."

(U) Poe made cryptanalysis an important aspect of his famous short story "The Gold Bug"; the protagonist solves an enciphered message which turns out to be directions to finding buried pirate treasure. In addition, Poe, as an author and editor, published a series of articles on cryptology and secret writing systems.

(U) Whatever his claims as a theorist, Poe proved himself rather limited as a practitioner. According to his recent biographer, Kenneth Silverman, in 1839-40, as editor of a family newspaper entitled "Alexander's Weekly Messenger", Poe challenged his readers, inviting them to send encrypted messages and promising to solve them all. The offer had a catch, however: Although the readers could employ symbology as well as conventional letters, the messages had to be enciphered in a single alphabetic substitution system; he rejected messages enciphered by any other method. With this stipulation, it is hardly surprising that Poe achieved a high rate of success against his readers' entries or that he often reprinted them with the solutions--together with a boast of his speed and skill in solving them.

(U) Rather than being one of the best informed cryptologists of his day, Poe's total pool of knowledge, Silverman points out, seems to have been gleaned from several encyclopedia articles on cryptology. Silverman concludes that "he was entirely a novice, as the still more naive readers of "Alexander's" failed to realize."

[David A. Hatch, Director, Center for Cryptologic History, [redacted]

[redacted]

****

//////////

10. EDITORIAL CORNER

(b)(3)-P.L. 86-36

If you have a relatively short technical treatise, or anything you would like to have considered for inclusion in future issues, please submit it to any member of the editorial board or any of our office POCs.

PLEASE paragraph classify each item submitted, and USE ASCII FORMAT!

A reminder that anonymity may be requested for Action Line items - in fact, you may mail them in hardcopy form to any member of the editorial board or any of our office representatives.

We would very much like this newsletter to represent a broad cross-section of the CA community - we need some more volunteers to help us, however. Perhaps you would like to work on one of the topics in this issue, or perhaps there is another topic which you think should be included in future issues. Either way, we would like your input, and help, so give one of us a call. The more people who divide up the work, the less burden on any one person.

##########

NOTE: We MUST receive any submissions for the December issue by 25 Nov.

[redacted]

##

EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum

[redacted] NCS

OFFICE Reps

[redacted]

(b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

[redacted]

TOP SECRET//COMINT

(U) POC: [redacted] info
(U) Last Modified: 11/04/2002 13:04:51
(U)PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
December 1994

Season's Greetings and Best Wishes for a Happy New Year

##########
//////////

~~//FOUO~~

(U) TABLE OF CONTENTS:

1. Perspectives in CA - [redacted]

2. KRYPTOS Society
   a. New Distinguished Members Announced
   b. Literature Competition Winners
   c. Peter Jenks Community Service Award Given

3. Calendar of Events

4. Word from the CACP
   a. CPEB Change
   b. Panel Updates

5. Technical Health
   a. Conference Schedules
   b. ACE Call for Abstracts
   c. CMI and MATHFEST

6. Community Service
   a. CLA Cinema Presentations
   b. E-Mail to Second Parties
   c. NSA Science and Engineering Presentation
   d. CAL Foreign Films Available

7. Puzzles and Problems

8. Literary/Historical Tidbit

9. Editorial Corner

##########
//////////

1. PERSPECTIVES IN CA

(~~TS-CCO~~) Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice, and we alternate between Seniors from within Z and Seniors outside Z. This month we are

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

pleased to print the thoughts of [redacted] Chief Z2.

The Director of Central Intelligence identifies Cryptanalysis as NSA's core discipline and key to the future of SIGINT effectiveness. Recognition of the importance of our profession by our most senior leadership is both flattering and frightening. It instills great pride among the CA community. But at the same time, it places a tremendous responsibility upon us to sustain our record of achievement upon which SIGINT relies.

Why is CA important? The answer is quite simple. Our targets use codes and ciphers to protect their most important communications. When we are able to decrypt these signals, we are able to penetrate the target. Our customers now have access to first-hand information: the target's diplomatic or economic negotiating position; its military plan of attack; or its own plans for intelligence activities. Throughout the course of history, we have demonstrated that intelligence based on decrypted communications does, in fact, save lives. What greater impact can we possibly expect to have?

But, can we live up to the responsibility which the DCI has put upon us?

Today we expend a lot of energy questioning ourselves. We worry that we are not trained to deal with a revolutionized telecommunications system. We are chagrined that we are unable to bring in larger numbers of interns. We are fearful of the effects of a shrinking budget. We are frightened by the proliferation of sophisticated crypto devices. All of these are valid concerns. Yet in fact, we have made some progress in dealing with them. We do have new courses available to the work force. We have learned to apply classic crypt techniques to recovering elements of modern communications technology.

Yes, we have goals remaining to be met. But let's be positive: emphasize what we can do - and do it. We may not solve every problem which we attack; but we'll probably make far more progress than any of us imagines possible today. For those challenges without an apparent course of action, let's team together to design creative solutions. And in doing so, let's respect every individual and organizational role in the intricate cryptanalytic process.

One of our greatest assets is our confidence. We believe in ourselves and in our ability to solve hard problems. We have a dedicated, bright work force. We have invested in state-of-the-art tools. We have fun. We share knowledge. We've known one another for years. We tolerate - even enjoy - our reputation as eccentric. We are a unique community in this Agency. Let's take pride in these strengths and apply them to the challenges.

(b)(3)-P.L. 86-36

****
//////////

2. KRYPTOS SOCIETY

(U) Over [redacted] people attended the annual KRYPTOS Society Luncheon at the Officers' Club. As is customary, the newest Distinguished Member inductees, and the recipients of the Literature Contest Prizes were announced, as well as the first winner of the Peter Jenks award.

****

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

AND THE WINNERS ARE ....

a. Distinguished Members - The KRYPTOS Society inducted three new members this year, and we have inlcuded biographical sketches of each.

[redacted]

[redacted] (b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

b. ~~(TSC)~~ Literature Competition Winners

First Prize: [redacted]

Second Place Tie: [redacted]

(b)(1)
(b)(3)-P.L. 86-36

and

[redacted]

(b)(3)-P.L. 86-36

[redacted]

Honorable Mention Tie: [redacted]

and

[redacted] (b)(1) (b)(3)-P.L. 86-36

****

c. First Peter Jenks Community Service Award Given

(U) Following are the words of [redacted], outgoing Chairman of the CACP, as he announced the first recipient of this new award granted in recognition of exceptional service and contribution to the CA Community.

"We are here today to honor two people, one, unfortunately, in memory only. Peter Jenks was a most unusual man, one who defied definition, who lived by his own rules, by his own wits. Though he was widely admired, none would try to emulate him, and his eccentricities ensured that he would remain unique in our memories.

(b)(3)-P.L. 86-36

In our search for an individual who, like Peter Jenks, has given so much of his life in the service of Cryptanalysis and cryptanalysts, one name stands out above the rest. Tireless, energetic, compassionate, generous --- these adjectives, which applied so well to Peter Jenks, also apply to the first recipient of the award which bears his name.

When the first Cryptanalysis Conference was convened last year, Floyd Weakley was selected by the Career Panel to make the opening remarks and to chair the ensuing discussion of the critical issues which confronted our profession. Floyd is the principal architect of the Technical Track program in Cryptanalysis, and has for many years prepared the exhaustive and extensive CA Report. He is a member of the Cryptanalysis Career Panel and a leader in the Kryptos Society. No one here has done more than Floyd in the development of our career field, and it is with great pride and humility that Fred and I present the first Peter Jenks Community Service Award to Floyd Weakley."

****
//////////

3. CALENDAR OF EVENTS

Dec 1	CMI Talk [redacted] (0930, Friedman)
Dec 7, 8	CLA Cinema "Journey of Hope", (OPS2B4118-1 1100)
Dec 8	NSA Science and Engineering Society Talk - "Optics for High Speed Computation" by [redacted] R&E Symposium Center 1000 a.m.
Dec 8	IAI Holiday Social [redacted] is POC)
Dec 12	Z2 Technical Forum (1300, OPS1, 2C086) "Z Data --- How Does It Get to Your Desk?" (briefing by Z Data Flow Managers, 1300-1400,

(b)(3)-P.L. 86-36

[redacted]

OPS1 room 2C086)

	Dec 13	IAI Talk, (1000-1100, OPS2B 4118-6) Mary McCarthy, NIO Warning, "The Intelligence Community's Responsibility to Warn in the 1990's"

PLAN AHEAD:

	Jan 7, 1995	Last day to USE-OR-LOSE Annual Leave
	Jan 9, 1995	Z Technical Forum
	Jan 18, 1995	BANCC (see CACP News)
***	Jan 25-26, 1995	1995 Cryptanalysis Conference (SRC)
	March 27-31, 1995	CARD (GCHQ)
	May 1-5, 1995	ACE (CCR Princeton)
	May 23-25, 1995	CA PQE
	Jun 5 - 9, 1995	CA-305
	June 1995	MATHFEST '95

*** - NOTE - THIS IS A CHANGE.

//

4. CACP NEWS

(U) (Late-breaking news as we "go to press" - [redacted] Z21, the former Chairman of the Career Panel, has been named temporary Acting Chairman until further notice, as [redacted] has been named by the Director to a special task force!)

(b)(3)-P.L. 86-36

a. (U) CA Panel Update

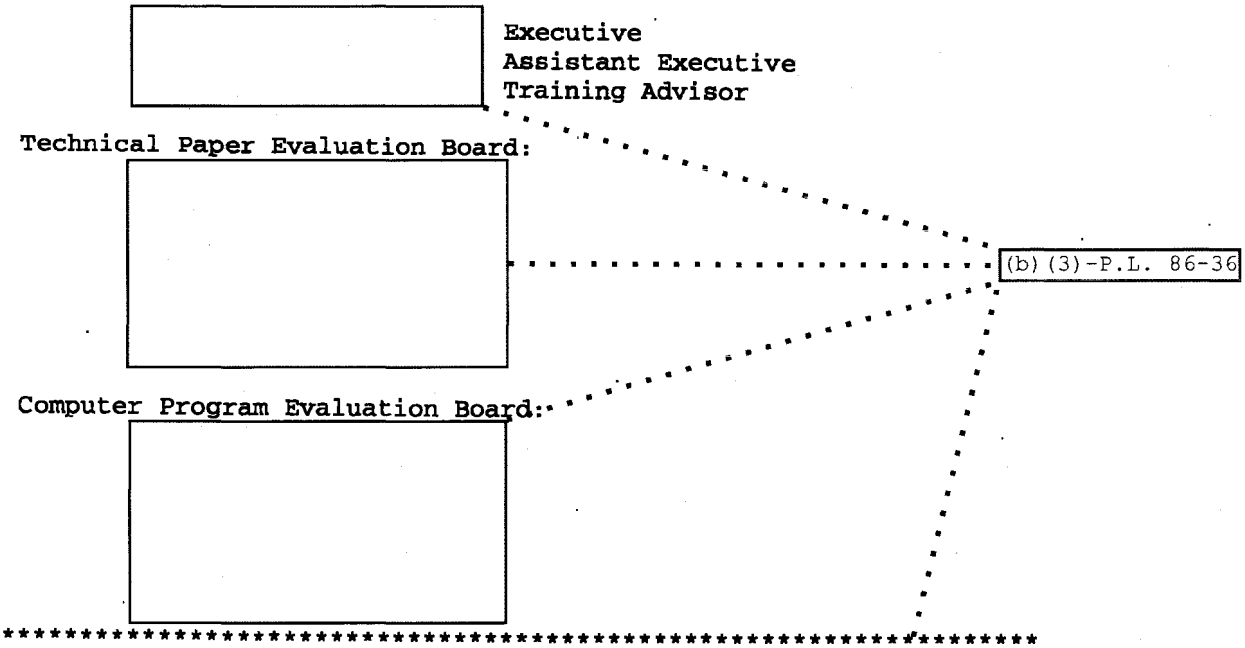
There have been several changes in the Panel and Boards. [redacted] has accepted a position on the Computer Program Evaluation Board. She will begin to attend meetings immediately and will officially replace [redacted] on 1 December 1994. [redacted] has accepted a position on the Technical Paper Evaluation Board. She will begin to attend meetings in December and will officially replace [redacted] on 1 January 1995.

Cryptanalysis Career Panel:

[redacted] Chairman

(b)(3)-P.L. 86-36

[redacted]



****
//////////

5. TECHNICAL HEALTH

a. (U) Conference Schedules -

Following is a list of some of the conferences coming up which might be of interest to the Z population -

Dec. 5-7: Washington, DC
SPONSORS: Technology Training Corp (TTC)
THEME: "Data Fusion" (and associated topics)
FEE: $825 - $1145 (depending on employment-status (e.g. Univ. or Govt.) and registration date)
ADD: Alan Friedman
TTC Seminars
Dept. DF
P.O. Box 3608
(3420 Kashiwa St.)
Torrence, CA 90510-3608
TEL: (310) 534-4871

****

1995:

Jan 8-11: Tucson, AZ (Ventana Canyon Resort)
SPONSOR: IEEE Communications Society
THEME: "Broadband '95 Workshop: Emerging Broadband Applications, Systems, Networks"
FEE: $945 to $1,045 (depending on membership-status and registration-date)
ADD: Judy Keller
IEEE Communications Society
345 E. 47th St.
New York, NY 10017-2394
TEL: (212) 705-8248
FAX: (212) 705-7865
E-MAIL: j.keller@ieee.org

Jan. 23-26: Washington, DC
SPONSORS: Network World
Federal Computer Week
Computerworld
THEME: "COMNET '95: Leading Communication into the Global Age"
FEE: not listed (but a $50 "Super Pass" to exhibits and to some sessions is free upon early registration)
ADD: COMNET '95
IDG World EXPO
Framingham, MA 01701-9699
TEL: 1-800-225-4698
1-508-879-6700
FAX: 1-508-872-8237
E-MAIL: comnet@idwec.com

Feb. 5-10: San Jose, CA
SPONSOR: not listed
THEME: "Digital Video Compression: Algorithms and Technologies 1995"
FEE: not listed
ADD: Jane Lybecker/Donna Rode
SPIE
P.O. Box 10
Bellingham, WA 98227-0010
TEL: (206) 676-3290
FAX: (206) 647-1445

****

b. (TSC) CALL FOR ABSTRACTS - ACE 95

The Annual Cryptomathematics Exchange, ACE, will be held the week of May 1-5, 1995, at CCR in Princeton, New Jersey. ACE is the premier conference for classified cryptomathematics. Those wishing to give a talk must submit a short abstract to an ACE representative by Friday, January 13, 1995.

The short abstract should be two pages, in soft copy ASCII, submitted to a committee member. Talks can be classified up to TOP SECRET CODEWORD and should not contain NOFORN or source-related material. Compartmented presentations will be allowed during afternoon parallel sessions.

Please note that talks given at ACE must be on topics that have been released to Second Parties and also to IDA (topics can be released for the purposes of presentation at ACE). Abstracts are generally sent to members of those organizations who are on the ACE committee. If you plan to submit an abstract, it is important to know whether it can be released to second parties and IDA.

****

c. CMI AND MATHFEST

The CMI council is actively making preliminary arrangements to host a festival in June which aims to bring together the entire mathematics community for a single day to exchange the major results of the past year. Unlike ACE, CARD, DATA DEMOD, etc. this meeting seeks to celebrate mathematics in all its forms at NSA, and to familiarize the CMI membership with the diverse applications of cryptomathematics being used and created at NSA.

The organizing committee envisions approximately sixteen 15-minute

talks spread over a full day. We expect the bulk of representation coming from Z, C, R, and W. As such, we are sending the formal announcement at this time to selected Office chiefs in these groups, seeking comments and suggestions on how to make this festival useful, enjoyable, and rewarding.

At this time please feel free to share the announcement at your own discretion, bearing in mind that the format remains flexible and no firm commitments beyond the date have been made.

For additional information, contact [redacted] via e-mail.

(b)(3)-P.L. 86-36

6. COMMUNITY SERVICE

a. (U) CLA Cinema presentation - JOURNEY OF HOPE (111 minutes) Turkish with English subtitles. This winner of the 1991 Oscar for Best Foreign Film is a passionate drama about a poor Kurdish couple who decide to make a better life for themselves and their seven children by moving to Switzerland from their native Turkey. Their dangerous journey is chronicled in this stirring film directed by Xavier Koller.

b. (U) E-Mail to Second Parties Changes

Agency changes to mail routing will result in the following address modifications. Old forms will not work after 30 November.

New addresses should read:

(b)(3)-P.L. 86-36

[redacted]
(England)
(Canada)
(Australia)
(New Zealand; not yet available)
(USA)

c. (U) The NSA Science and Engineering Society will sponsor a presentation by [redacted] from the National Security Agency Physical Science Laboratory at 10 AM on Thursday December 8th in the Research and Engineering Symposium Center. [redacted] a Senior Member of the Institute of Electrical and Electronic Engineering Society, will address -

"Optics for High Speed Computation".

This will include optical applications to high performance computers and to projects in both the SIGINT and INFOSEC areas.

All green and gold badge personnel are invited to attend.

d. (U) CLA Foreign Language Movies Available

The following is a current alphabetized list of CLA foreign language movies available for FREE USE. Call [redacted] if you want to borrow any:

(b)(3)-P.L. 86-36

[redacted]

1. Ashes and Diamonds (Polish/English subtitles)
2. Attila 74 (Greek/English subtitles)
3. Chocolat (French/English subtitles)
4. Come and See (Russian/English subtitles)
5. Commissar (Russian/English subtitles)
6. Hey Babu Riba (Serbo-Croatian/English subtitles)
7. JuDou (Chinese-Mandarin/English subtitles)
8. June Night (Juniatten) (Swedish/English subtitles)
9. Raise The Red Lantern (Chinese-Mandarin/English subtitles)
10. Ramparts of Clay (Arabic/English subtitles)
11. Red Sorghum (Chinese-Mandarin/English subtitles)
12. Terra Em Transe (Portuguese/English subtitles) *
13. The Home and the World (Bengali/English subtitles)
14. The Lady With the Dog (Russian/English subtitles)
15. The Official Story (Spanish/English subtitles)
16. The Red and the White (Hungarian/English subtitles)
17. The Shadow by the Road (Chiec Bong Ben Duong) (Vietnamese/French and Chinese subtitles)
18. This Land Is Ours (Hausa/English subtitles)
19. Two Women (Italian/English subtitles)
20. Wake Up Vasili (Xipna Vasili) (Greek/no subtitles)
21. Yol (Turkish/English subtitles)

*It says Spanish on the movie jacket but is in Portuguese. The last twenty minutes of this one are missing as well. We at CLA believe in truth in advertising.

As you can see, we have a decent library. However, we are not too proud to beg for more movies. If you have any that you can bear to part with, then you can once again give [redacted] a call at [redacted] Thank you.

****
//

7. PUZZLE

(b)(3)-P.L. 86-36

(U) Insert a different group of 3 letters into each of the "words" below so as to form 2 real words - the 3 letters you insert will be the last three letters of one word and the first 3 letters of the other: No rearrangement of the given letters is permitted. Once you have determined the correct 3 letters for each word in a set, you may put them together to form a single 9-letter word. Again, no rearrangement of letters is permitted.

Example: MARED Insert "BLE" to form "MARBLE" and "BLEED"
FORAISE Insert "MAL" to form "FORMAL" and "MALAISE"
PTHER Insert "LEA" to form "PLEA" and "LEATHER"

The groups "BLE", "MAL" and "LEA" may be assembled to form the word "MALLEABLE".

HUGER	SHOO	GILER	CRELIER	BASENT	CATLE
CALIMIT	PANAST	SHROUND	GERLET	MENMENT	INSAL
PATICE	COROBE	SPHODOX	CORLY	CLQMIN	ARCKLE

[redacted]

****
//////////

8. LITERARY/HISTORICAL TIDBIT

The Rewards of COMINT

(U) During the Civil War, both Union and Confederate forces engaged in the intercept of telegraph messages from the other side, often profiting by the intelligence derived from reading plain text or decrypting messages sent in code or cipher. In late 1864, as General Ulysses Grant was at the gates of Richmond, the Confederates received special benefits from what one source calls the "most successful wire tapping of the war."

(U) For six weeks, a Confederate operator maintained a continuous tap on General Grant's telegraph line to the War Department. Despite the longevity of the tap, it is believed that none of Grant's encrypted cables were decrypted by the Confederates (or "translated", as they sometimes called it in those days).

(U) On 12 September, however, the Quartermaster in Washington sent a plaintext message to Grant's forces requesting a guard to meet 2,486 head of cattle due to arrive the next day at a landing at nearby Coggins Point. This was good news for the Confederate Army, which was nearly always short of food supplies and drastically short of meat. A large body of Confederate cavalry traveled by a roundabout route to Coggins Point, where they captured the beef along with 300 Union soldiers, 200 mules, 32 wagons, and 40 telegraph construction workers.

(U) Thanks to the telegraph intercept, for the first time in months if not years, the Confederates ate well, having captured about 40 days' worth of supplies.

(SOURCE: William R. Plum, "The Military Telegraph during the Civil War in the United States:, Vol II" - submitted by David Hatch, CCH)

****
//////////

9. EDITORIAL CORNER

If you have a relatively short technical treatise, or anything you would like to have considered for inclusion in future issues, please submit it to any member of the editorial board or any of our office POCs.

PLEASE paragraph classify each item submitted, and USE ASCII FORMAT!

A reminder that anonymity may be requested for Action Line items - in fact, you may mail them in hardcopy form to any member of the editorial board or any of our office representatives.

We would very much like this newsletter to represent a broad cross-section of the CA community - we need some more volunteers to help us, however. Perhaps you would like to work on one of the topics in this issue, or perhaps there is another topic which you think should

be included in future issues. Either way, we would like your input, and help, so give one of us a call. The more people who divide up the work, the less burden on any one person.

##
NOTE: We MUST receive any submissions for the January issue by 21 Dec.
##

EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum

[redacted] NCS

OFFICE Reps

[redacted]

(b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2, DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR" DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

[redacted]

TOP SECRET//COMINT

(C) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:17
(U) PE EXTERNAL PAGE

[redacted] (b)(3)-P.L. 86-36

****
* TALES OF THE KRYPT *
****

January 1995

##########
//////////

(FOUO) TABLE OF CONTENTS:

1. KRYPTOS Society
   a. First Annual Breakfast Affair for Newly Certified Cryptanalysts
   b. KRYPTOS Society Membership Renewal

2. Calendar of Events

3. Word from the CACP
   Postponement of Annual Cryptanalysis Conference

4. Technical Health
   a. SES Symposium
   b. ComNet 95

5. Technical Article
   The Challenge of Bulk Enciphered Signals

6. Community Service
   [redacted]-The People Behind the Name

7. Puzzle [redacted] (b)(3)-P.L. 86-36

8. Literary/Historical Tidbit
   a. Hobbyist's Guide to COMINT Collection and Analysis
   b. Dr. Dobb's Journal

9. Editorial Corner

##########
//////////

1. (FOUO) KRYPTOS Society

a. First Annual BANCC

The Cryptanalysis Career Panel and the KRYPTOS Society are hosting the first annual BANCC (Breakfast Affair for Newly Certified Cryptanalysts) on 18 January 1995 from 0800-1000 in the Canine Suite. Join your friends and co-workers and celebrate with all of the honorees:

[redacted] (b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

[redacted]

Breakfast Buffet: Fruit Juice, Fresh Fruit Cup, Scrambled Eggs, French Toast, Bacon, Biscuits, Toast, Coffee/Tea. Cost: $6.00
R.S.V.P. Deadline: 12 January 1995 to one of the following POCs:

[redacted]

b. Kryptos Society Council

The current KRYPTOS Society Council members are: (b)(3)-P.L. 86-36

President [redacted]
President-elect
Secretary [redacted]
Treasurer
Member-at-large
Member-at-large
Member-at-large
Member-at-large Floyd Weakley

c. Kryptos Society Membership Renewal

It's the beginning of a New Year, why not join us? We need your membership and your input to give voice to the cryptanalysts in our community now and in the future. This is an excellent chance for networking at all levels. To join, just fill out the attached application, and send it, and $5.00 to -

[redacted]

**** KRYPTOS MEMBERSHIP APPLICATION DUES: $5.00 (Annually)****

MEMBERSHIP YEAR: 1995 ( ) NEW ( ) RENEWAL

NAME:_____ DATE: _____

SECURE PHONE: _____ NON-SECURE: _____

ORG: _____ BLDG: _____

[redacted]

INTERESTED IN CHAIRING A COMMITTEE? ____YES ____NO

INTERESTED IN WORKING ON A COMMITTEE? ____YES ____NO

CHECK COMMITTEES OF INTEREST TO YOU:

____ CRYPTANALYTIC LITERATURE ____ MEMBERSHIP

____ DISTINGUISHED MEMBERS ____ PUBLICITY ____AWARDS

____ PROGRAMS ____ NEWSLETTER ____ RETIRED MEMBERS

~~~~~~
****
//

2. (FOUO) CALENDAR OF EVENTS

Jan 7	Last day to USE-OR-LOSE Annual Leave
Jan 9	Z Technical Forum (1300-1400, OPS2B, room 4118-2B6)
Jan 12	CMI Talk "The President's Address" by [redacted] (0930-1100, Friedman Auditorium)
Jan 17	SES Symposium Talk "A Military-Technological Revolution" by General Welsh, President and Chief Executive of IDA (1000, R&E Symposium Center) (see Technical Health)
Jan 18	First Annual Breakfast Affair for Newly Certified Cryptanalysts (0800-1000, Canine Suite)
Jan 18	NEWSMAGAZINE Talk "The State of the Agency" by Vice Admiral J. M. McConnell, Director, NSA (1000-1100, Channel 50 in OPS, Channel 21 in FANX II; also broadcast live in Course Center B, room A1B045, FANX II.) Tune-in and call-in your questions. Dial: [redacted]
Jan 23-26	ComNet 95 (Washington Convention Center) (see Technical Health)

PLAN AHEAD:

	March 27-31, 1995	CARD (GCHQ)
**	March 29-30, 1995	1995 Cryptanalysis Conference (SRC)
	May 1-5, 1995	ACE (CCR Princeton)
	May 23-25, 1995	CA PQE

(b)(3)-P.L. 86-36

[redacted]
~~~~~~

** June 5 - 9, 1995 CA-305

June 1995 MATHFEST 95

(** NOTE - this is a change.)

****

//////////

3. (~~FOUO~~) Word from the CACP

Annual Cryptanalysis Conference Date Changed

In October, the Cryptanalysis Career Panel began consultations with senior Z managers to solicit their views on the future cryptanalytic needs of the Agency. Using the results of this process, and recommendations from the first two cryptanalysis conferences, we are developing a course of action designed to ensure our technical viability into the future. With the January conference date fast approaching, and our work not yet complete, we have decided to move the conference to 29 and 30 March, 1995. We certainly hope the change does not prove to be an inconvenience, for we expect the extra time devoted to planning to be very beneficial.

[redacted]
Acting Chairman, Cryptanalysis Career Panel

****

//////////

4. TECHNICAL HEALTH

a. (~~FOUO~~) SES Symposium (b)(3)-P.L. 86-36

The NSA Science and Engineering Society (SES) will sponsor a presentation by General Larry Welsh (USAF retired) at 10 AM on Tuesday, January 17th in the Research and Engineering Symposium Center. General Welsh is the President and Chief Executive Officer for the Institute for Defense Analysis (IDA). Among its many functions, IDA operates the Supercomputing Research Center in Bowie and the Centers for Communication Research at Princeton and La Jolla for NSA. The title of General Welsh's talk is

"A Military-Technological Revolution".

He will address the end-to-end combat information system from intelligence collection to combat direction, how technology has produced revolutionary changes in military capabilities and how our intelligence superiority supports the utilization of these capabilities.

All green and gold badged personnel are invited to attend.

****

b. (U) ComNet 95

ComNet 95 will be held 23-26 January 1995 at the Washington Convention Center. According to an advertisement in a recent issue of Telecommunications magazine: "Explore leading-edge technologies and emerging business applications that are the building blocks of the global enterprise from ATM, Frame Relay and FDDI, to multi-media, videoconferencing, wireless, digital convergence and the Internet." This is an opportunity to gather technical

[redacted]

literature, view demonstrations, and talk to technical experts in commercial telecommunications. Admission to the exhibition hall is free. For more information, call 800-225-4698.

****
//////////

5. TECHNICAL ARTICLE (b)(3)-P.L. 86-36

~~(FOUO)~~ The Challenge of [redacted]
by [redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

[redacted]

****
//////////

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

6. COMMUNITY SERVICE

(b)(3)-P.L. 86-36

(U) [redacted]-The People Behind the Name
by [redacted]

~~(S)~~ Many cryptanalysts are aware that [redacted] but some may not know that this [redacted] is named for its three inventors: [redacted] These distinguished members of the cryptanalytic community have made many contributions to our field, as well as to academia, over the years.

[redacted]

(b)(3)-P.L. 86-36
(b)(6)

[redacted]

(b)(3)-P.L. 86-36

[redacted]

(U) Thus the [redacted] has more to its name than first meets the eye.

(b)(3)-P.L. 86-36

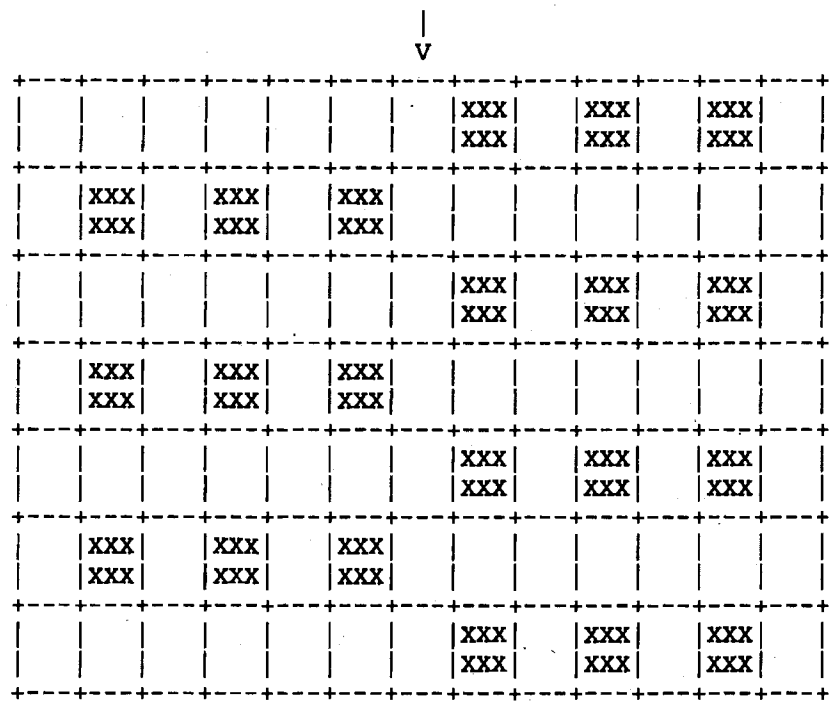
7. Puzzle

a. Solution to last puzzle:

hu MAN ger	sho ALS o	gi ANT ler
cali PER mit	pana CHE st	shr IMP ound
pat ENT ice	co MIC robe	sp ORT hodox
PERMANENT	CHEMICALS	IMPORTANT
cre ATE lier	ba CON sent	ca PES tle
ger BIL let	men TOR ment	ins IDE al
cor RAL ly	clo VER min	arc TIC kle
BILATERAL	CONVERTOR	PESTICIDE

b. January KRYPTOS Puzzle

The Light Fantastic by [redacted]



(b)(3)-P.L. 86-36

The following cryptic clues all lead to 7-letter words which are to be entered into the diagram above. The clues are given in no particular order, and the solver must determine which word goes where. The word in the center column (indicated by the arrow) is unclued: you must determine what it is.

A. Lodge member, returning after the first victory, to act as a star.
B. It's liked by all, turning up in extreme.
C. Untidy trunk emptied, but just a section.

[redacted]

D. Burn returned book draft, having come first.
E. Late returns having earl leading nurse to the last.
F. Mistakenly rush mob figure.
G. Turns on to act as carriers.
H. Alternate route carries little one to remote part.
I. Impossible dream to note that man comes ahead of time.
J. Crown used once or twice, initially.
K. Plant to be, to a point, without framework.
L. He can't believe what he sees: King in filthy surroundings.
M. Hold up: no twitching is automated.

For those of you who may be unfamiliar with the cryptic style of clueing, each clue consists of two parts: a more or less straightforward definition of the solution word; and a word-play which may involve anagrams, synonyms, clueing parts of the solution word separately, or any of a multitude of other techniques. Either part (the definition or the word-play) may come first, but there may be no overlap of parts. A 'connector' word or phrase ("is", "for", "makes", "goes to", etc.) may sometimes be used in the clue to act roughly as an `equals sign' between the parts. Here is an example which employs several clueing tricks. (It is traditional in cryptics to give the number of letters in the solution word. In this puzzle, all words will be 7 letters long, so this help is omitted.)

CLUE: Fixed ten damaged trails for each fellow. (9)
ANSWER: PERMANENT

The definition is "Fixed". "Ten damaged" is a common convention that suggests that the word "ten" should be anagrammed. (All anagrams will have a clue word such as this. Look for "broken", "confused", "muddled", etc.) "Ten" anagrammed is "ENT". "Trails" suggests that this part of the word comes after whatever is clued next. "For each fellow" can also be expressed as "PER MAN". So the solution is "PER MAN ENT".

****
//////////

8. LITERARY/HISTORICAL TIDBIT

a. (U) Book Review "Hobbyist's Guide to COMINT Collection and Analysis"

(TSUO) Browsing the INTERNET, an alert reader spotted a review of a book of possible interest to KRYPTOS members: "Hobbyist's Guide to COMINT Collection and Analysis" by Tom Roach. This book is in the NSA Main Library (Circulating) Collection:

Author: Roach, Thomas B.
Title: Hobbyist's Guide to COMINT Collection and Analysis /
Publication info: San Jose, CA : Tom Roach, c1994.

CALL NUMBER - JK468.I6 R53 1994 MAINCIRC

(U) Here are some excerpts from the book review by a non-Agency subscriber, Edward Anderson, in INTERNET article 11e@ixnews1.ix.netcom.com, Anok@ix.netcom.com, on 8 December 1994:

"The Hobbyist's Guide to COMINT Collection and Analysis breaks new ground here, since it provides information on how easily the reader can

collect and analyze COMINT. It turns out this can be done with radio receivers and "decoder" boxes which are easily purchased on the open market. The book reveals some of the very interesting Russian messages Mr. Roach has received using a shortwave receiver and "decoder" while sitting in the comfort of his den. And what a bizarre catch he reveals. The messages range in subject matter from the deliberate canning of fish tainted by toxic waste, to an "upper air weather" message broadcast from a Russian trawler sitting off Vandenberg AFB. The Russian vessel was monitoring tests of United States' anti-missile missile launches from Vandenberg to Kwajelein.

The book even includes intercepts, and technical descriptions of four distinctly different types of KRIPTOGRAMMA messages. These are messages which use special Russian encryption methods (still in use). The messages are sent by both Russian trawlers (who catch a lot more than fish!) and Space Event Support Ships (SESS). You are even instructed in how to learn when, and where, the next Russian ICBM shot will impact in the icy waters off the Kamchatka peninsula. You learn how to find the proper radio frequency to monitor ship traffic in the Middle East. As a convenience, the book comes with a spiral metal binder so it can lay flat on the desk of the home COMINT collector deciphering the latest Russian "20101" message. Lest you believe only the Russians provide material for the hobbyist, the author reveals how he intercepted a U.S. military classified message accidentally sent in the clear. The techniques discussed in this book can be applied to almost any sort of radio traffic.

The reader is provided examples of various Russian "numbers" messages, which at first glance may appear "encrypted". Mr. Roach gives the exact methodology which resulted in one such message's "decryption". A whole chapter is devoted to teaching the uninitiated how to "decipher" similar messages on their own. The means by which the Internet can be used to allow hobbyists to share information, get translations, and combine intercepts to gain greater insight is described. According to the author, you don't even need to be able to speak Russian to get the basic meaning of many of the Russian messages that are still being broadcast. Mr. Roach stresses that COMINT, even at this level, provides a real insight into just what extent, and how successfully, "capitalist" ventures are developing in the "new" Russia. In fact, Mr. Roach has published a second book, Hobbyist's COMINT Russian Radioteletype Dictionary, to assist those who actually take up the hobby."

****

b. (U) Dr. Dobb's Journal

(U) The January 1995 issue of Dr. Dobb's Journal contains two articles of interest to cryptologists:

1. Page 123 - The GOST Encryption Algorithm, by Bruce Schneier
This algorithm was used by the former Soviet Union, possibly for the civilian market. The analysis does a comparison to DES.

2. Page 146 - The RC5 Encryption Algorithm, by Ronald L. Rivest
Description of the named algorithm.

(b)(3)-P.L. 86-36

(FOUO) [Note: [redacted] of the KRYPTOS Newsletter Editorial Board, advises that Dr. Dobb's Journal may be found in the NSA Main Library as follows. As you go towards the newspaper reading area, it is in the second section on the right (aisle 60), the next to the bottom shelf (alphabetically under D).]

****

[redacted]

//

9. EDITORIAL CORNER

If you have a relatively short technical treatise, or anything you would like to have considered for inclusion in future issues, please submit it to any member of the editorial board or any of our office POCs.

PLEASE paragraph classify each item submitted, and USE ASCII FORMAT!

A reminder that anonymity may be requested for Action Line items - in fact, you may mail them in hardcopy form to any member of the editorial board or any of our office representatives.

We would very much like this newsletter to represent a broad cross-section of the CA community - we need some more volunteers to help us, however. Perhaps you would like to work on one of the topics in this issue, or perhaps there is another topic which you think should be included in future issues. Either way, we would like your input, and help, so give one of us a call. The more people who divide up the work, the less burden on any one person.

##
NOTE: We MUST receive any submissions for the February issue by 15 Jan.
##

EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum

[redacted]

OFFICE Reps

[redacted]

(b)(3)-P.L. 86-36

[redacted]

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

(b)(3)-P.L. 86-36

[redacted]

9/23/2010

TOP SECRET//COMINT

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:17
(U)PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
February 1995

##########
//////////

(FOUO) TABLE OF CONTENTS:

1. CA Perspective

2. KRYPTOS Society
   a. KRYPTOS
   b. Membership Application
   c. Talks on Tape

3. Calendar of Events

4. Word from the CACP

5. Technical Health
   a. "It Was the SAWUNEH of 94"
   b. Signals Development Conference

6. Community Service
   a. [redacted] Algorithm and Its Inventor
   b. Center for Cryptologic History
   c. Math News

7. Puzzles and Problems
   a. Solution to January Puzzle "The Light Fantastic"
   b. Solution to November PROBLEM OF THE MONTH
   c. February PROBLEM OF THE MONTH

8. Literary/Historical Tidbit - [redacted]

9. Action Line

10. Editorial Corner

(b)(3)-P.L. 86-36

##########
//////////

1. (FOUO) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to print the address [redacted], Acting Chairman of the CACP, delivered at the recent Breakfast Affair for Newly Certified Cryptanalysts.

To the Newly Certified Cryptanalysts:

First I'd like to join with your colleagues and friends to congratulate you on your certification as cryptanalysts. We senior members of the cryptanalytic community are honored that you have chosen to associate yourselves with us and to put your shoulders (figuratively) and your minds alongside ours in the struggle to attain cryptanalytic knowledge.

It is more difficult to be a cryptanalyst now than ever before in our history. Our field has come of age. All the easy problems have been solved. To accept the mantle of cryptanalyst is to subject yourself to a career addressing difficult, often impossible, questions. The rewards are few and come seldom. Why do people like yourselves, who have so much to offer, choose such a demanding profession?

I chose cryptanalysis, as you did, because I love an intellectual challenge. I stayed in cryptanalysis, as I hope you will, because I enjoy the stimulating company of the other Agency professionals who have selected this uncompromisingly difficult

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

vocation.

We come from many backgrounds: geographically, academically, and ethnically. In the past months I have heard some interesting stories about several of you! That may be a trait common to cryptanalysts --- we are not dull people! We enjoy a variety of activities: some athletic, some intellectual, some social, ... We take great pleasure in our outside lives to compensate for the disappointment which comes so commonly to those who choose to test themselves daily on almost intractable problems.

But cryptanalysis is changing rapidly. The new modes of communication will force us to learn some new techniques and to discard others. This will make for exciting times, and you couldn't be in a better position. Whenever new methods are introduced, there will be errors and misunderstandings which will compromise seemingly secure cryptologics. The ablest among you will find and exploit these blunders and will achieve fame (at least internally). The successful cryptanalyst keeps trying, probing, testing, looking for some oversight which will confer enough of an advantage to permit first a small success, then a larger triumph, and finally the conquest of the seemingly impregnable fortress.

We oldtimers see in you the analysts who will replace us, who will rise above us, who will perform tasks we had thought to be impossible. We couldn't be prouder at the prospect of passing to you the responsibility for success in the enterprises we share. Some of us will get to work with some of you, to teach you, and to learn from you. As we increasingly rely upon you to solve the toughest problems, it is comforting to know that your ability, your preparation, and your determination will maximize our probability of realizing success.

We welcome you to our Community. We need your skill. Today's problems are too difficult for individuals to solve. Inspiration will still be welcome, of course, but maybe more important will be the ability to work together, to pool our communal strengths to overcome our individual weaknesses. You are our investment, our future. We will work with you to enhance your skills, and you will inspire us with your achievement. We must be partners, because each of us needs the other.

The KRYPTOS Society and the Cryptanalysis Career Panel work to bring cryptanalysts together. We are overwhelmingly introverted, and some of us are uncomfortable in social situations. Nevertheless, it is only through cooperation that cryptanalysts, and Cryptanalysis, will succeed. We thank the KRYPTOS Society for sponsoring this breakfast, and we welcome you as colleagues. Congratulations, cryptanalysts!

****

2. (TSUC) KRYPTOS Society

a. K R Y P T O S

The KRYPTOS membership drive is now underway. Perhaps you are asking just what is the Kryptos Society and why should you join?

The KRYPTOS Society was founded in 1981 to promote interest in cryptanalysis, to provide a focal point for fields of common interest to NSA cryptanalysts, and to promote continued excellence in professional cryptanalytic activity throughout the cryptologic community.

KRYPTOS sponsors briefings on topics related to cryptanalysis on both historical and specific current projects at its quarterly meetings and at other times during the year. This year KRYPTOS and the CACP sponsored the first annual Breakfast Affair for Newly Certified Cryptanalysts (BANCC). It was considered to be a resounding success and will be continued next year. Last May, KRYPTOS organized a luncheon at the National Cryptologic Museum which included a presentation by [redacted] on the Polish solution of the Enigma machine. Following the luncheon, individuals viewed the museum exhibits at their own pace, vastly aided by a cadre of knowledgeable guides. This event was also well-received and similar events are planned in the future. We hope to have quarterly events, in addition to our technical talks, throughout the year.

(b)(3)-P.L. 86-36

KRYPTOS recognizes sustained excellence in the cryptanalytic field through selection of Distinguished Members. It also sponsors an annual

[redacted]

literature contest and awards cash prizes. In the fall, we hold an annual luncheon for members and guests. At this event, a highlight of the KRYPTOS year, everyone gathers at the Officers' Club to enjoy lunch, socializing, and networking with new and old friends. It is during this event that KRYPTOS collectively recognizes professional achievement in our field. We hope to plan additional social events during the year. Any ideas for briefings or future events? Let one of our Council members know.

Join us! We need your membership and your input to give voice to the cryptanalysts in our community now and in the future. This is an excellent chance for networking at all levels. To join, just fill out an application and send it and $5.00 to [redacted] or any of the council members listed below:

President [redacted]
Secretary
Treasurer
Member-at-Large
Member-at-Large
Member-at-Large
Member-at-Large Floyd Weakley

---

b. KRYPTOS Membership Application

**** KRYPTOS MEMBERSHIP APPLICATION DUES: $5.00 (Annually)****

MEMBERSHIP YEAR: 1995 ( ) NEW ( ) RENEWAL

NAME:_____ DATE: _____

SECURE PHONE: _____ NON-SECURE: _____

ORG: _____ BLDG: _____

SID & HOST: _____

INTERESTED IN CHAIRING A COMMITTEE? ____YES ____NO

INTERESTED IN WORKING ON A COMMITTEE? ____YES ____NO

CHECK COMMITTEES OF INTEREST TO YOU:

____ CRYPTANALYTIC LITERATURE ____ MEMBERSHIP

____ DISTINGUISHED MEMBERS ____ PUBLICITY ____AWARDS

____ PROGRAMS ____ NEWSLETTER ____RETIRED MEMBERS

(b)(3)-P.L. 86-36

---

c. KRYPTOS TALKS AVAILABLE ON VIDEO

~~(TSC)~~ We have collected a number of tapes from previous KRYPTOS Talks, and we will be making them available through the Z Technical Library. If you have some of the old ones, please forward them to [redacted] We will update the list as we receive more tapes, and encourage you to borrow them, perhaps even arrange a brown-bag lunch around them, so that others may enjoy them too.

Collection of KRYPTOS Talks Available on Tape

Jan 95	~~(TSC)~~	[redacted]
Dec 94	(U)	The Harry Hantman Story
Jun 94	~~(SCC)~~	[redacted]
Apr 94	~~(SCC)~~	Harry Hoover Farewell Address
Mar 94	~~(SCC)~~	[redacted]
Sep 93	~~(TSC)~~	A Short Tale of a Long Cycle

(b)(3)-P.L. 86-36

[redacted]

Nov 92	(~~TSC~~)	History of a Successful Diagnosis
Sep 92	(~~TSC~~)	The SUNS Shine on a [redacted]
Jun 92	(~~TSC~~)	Classmate and Longshore (Technology for CA in the Field)
Nov 91	(~~TSC~~)	Just the FAX
Sep 91	(~~TSC~~)	Analysis of a Computerized Code
Jun 91	(~~TSC~~)	Superenciphered Systems
not dated	(UNC)	Cryptography in the Vineland Map

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

****
//////////

3. (~~TSCQ~~) CALENDAR OF EVENTS

February 15	[redacted] Telecommunications Technology Forum 1994/1995 Awareness Seminar Series Talk "International Networks & Gateways" by [redacted] (0800-1500, Friedman Auditorium)
February 16	IAI Talk "Russia's Winter of Discontent" by George Kolt, NIO for Russia and Eurasia (0930-1030, OPS2B, Room 2B4118-6; seating limited to 60 persons, IAI members have priority until 0925)
February 17	CLA Talk "The Political Aspects of the Gulf War", [redacted] (9A135, "1300)"
February 28	KRYPTOS/CMI Social at the "Last Chance" (1730-1930) (POC is [redacted])

(b)(3)-P.L. 86-36

(b)(6)

PLAN AHEAD:

March 2	CMI Talk (Friedman, 0930)
March 13	KRYPTOS Talk - Subject to be Announced (Friedman 1300-1500)
March 16	CLA/IAI [redacted] Baltimore Council Foreign Policy (9A135 1300)
March 16-19	3rd International Conference on Telecommunication Systems Modelling and Analysis (Nashville, Tenn.; 615-322-3694)
March 22-24	CISS `95, Conference on Information Sciences and Systems; (John Hopkins University; Baltimore, MD; (410) 516-7031)
March 28-31	IPCCC `95, Annual IEEE International Phoenix Conference on Computers and Communications; (Arizona State University; Phoenix, AZ; 602-965-7775)
March 27-31	CARD (GCHQ)
** March 29-30,	1995 Cryptanalysis Conference (SRC)
April 3-7	1995 Signals Development Symposium (Friedman Auditorium)
May 1-5,	ACE (CCR Princeton)
May 23-25,	CA PQE
** June 5-9,	CA-305
June	MATHFEST 95

(** NOTE - this is a change.)

****
//////////

(b)(3)-P.L. 86-36

[redacted]

4. (~~FOUO~~) Word from the CACP

a. This article is the second in a series reporting on follow-on activity from the working groups of the 1994 Cryptanalysis Conference. It would be helpful to have read the conference report before reading this article.

Reinventing CA: A Brave New World for the Career Field
by [redacted]

Last year's CA conference had as its central theme the role of the cryptanalyst in the modern, post-Cold War, post-reorg world. If you examine the conference speeches, you can pick out some of the issues which led the CACP to call for a hard look at our discipline. New technologies, austere hiring, an apparent contradiction in what outsiders and insiders considered to be cryptanalysis: these realities seemed to be pushing the classical cryppie into the margins of the cryptanalytic establishment, while the latter appeared to be becoming synonymous with the crypto-math community in the eyes of much of the Agency.

The 1994 conference organizers worked under the assumption that the ca vs. CA distinction which I defined in my speech was a valid one, and the conclusions that the "reinventing ca" working group reached seemed to support the perpetuation of that distinction. (For those for whom this is new, I defined "ca" as what someone professionalized in cryptanalysis is trained to do and "CA" as what Z group does.) In its report, the working group defined CA as "the diagnosis and exploitation of data which is, otherwise, not obviously intelligible." Then it went on to carve out a little niche for the "classical" cryptanalyst in diagnosis and exploitation, simultaneously stressing the importance of training in related fields. This is, perhaps, not surprising. We organizers stacked the conference with talks that showed how classically-trained cryptanalysts could be successful in what we termed "modern" cryptanalysis. We believed then that the way forward was to create a distinct identity for ca that would place it on an equal footing with the other disciplines that were involved in doing CA.

(b)(3)-P.L. 86-36

It took several months for the conference report to come out, and even longer for the Panel finally to put the report on the agenda for discussion. In the meantime [redacted] began his term as Panel chairman. [redacted] first initiative was for the Panel to go to the Office Chiefs and Chief, Z and ask their advice on what the CACP could do better to support the activities of their areas. These interviews were extremely enlightening. Another important thing happened during this period; the CA intern program looked like it was on the chopping block. With no hiring and all those empty billets, there was a distinct possibility that we might have to close down. Here, Dick Ruhl came to the rescue, suggesting that Z group might benefit by hiring computer scientists and engineers (these are, with mathematics, the relevant critical skills for CA) and training them through the CA intern program. There is still no hiring, but at least there is a plan.

By November it was clear that the Panel could no longer operate without a cogent working philosophy of the nature of cryptanalysis. The Panel had promised the community another conference in January, but as we wrestled with the issues confronting us, that conference seemed ill-timed and more and more irrelevant. At long last, in early December, the CACP held an offsite to synthesize the input we had received from the 1994 Conference, Z-group management, and from studies like the "Future of Cryptology". The conclusion of this day of soul-searching was to me as clicking the ruby slippers must have been to Dorothy: cryptanalysis is Cryptanalysis. We always had the power, but we had to find out for ourselves.

Simple as the concept is, the implications are far-reaching. Z-group cryptanalysis requires the efforts of people in many sub-disciplines. We, therefore, began to try to fashion a career field that would be equally as relevant to newly-hired mathematicians, computer scientists and engineers as to those in non-technical fields. In the ensuing months we have constructed new criteria for the field which attempt to ensure that every cryptanalyst will have a thorough grounding in the classical subjects: diagnosis, cryptography, related fields, but will also enable him to contribute in the areas for which his academic training has uniquely prepared him.

(b)(3)-P.L. 86-36

[redacted]

While last year's conference spotlighted how the classical cryptanalyst could move into areas of new technology, this year's gathering will focus on how to embrace diverse technical backgrounds to strengthen cryptanalysis. The new criteria for professionalization in cryptanalysis are a work in progress, and will be a major topic of the conference. Here is what they look like so far.

A number of the requirements will seem familiar on the surface. We will still require three years of creditable experience and we will still require a paper and a program. The omission of the PQE from this list is not accidental; an aspirant's grasp of essential knowledge will be assessed in other ways. We will require work experience in three core areas: exploitation, diagnosis and related fields. (When we say related fields we mean communications and collection). We will also require two elective tours, to be negotiated with the Panel execs. As an example, a mathematician might elect tours in attack development or algorithm design; an engineer might choose to do hardware reverse engineering or signals analysis; a computer scientist might work on CAPRI or study computer networks; a non-technical aspirant might delve into book-breaking or bit-stream analysis. We're not attempting to pigeon-hole anyone here - the mathematician could do book-breaking and the anthropology major algorithm design, the point is rather in the explicit inclusion of what was previously considered peripheral into our new vision of the career field.

Training requirements will be completely revamped, and this will necessitate a great deal of work in course development. Again, we envision a core of required courses and a wide choice of electives. The core will contain some new courses on which we hope to get started at the Conference: a related fields survey course, a "foundations of CA" course which will survey the most significant cryptographies extant, a new diagnosis course which I like to call "patterns of thinking", and a "topics in math, CS and engineering" course that will highlight the ideas in those fields with the most important implications for cryptanalysis. Some of our present required courses will become electives. Does everyone need to know how to solve a grille transposition? Probably not, just as we don't all need to program digital signals processing (DSP) chips, yet.

The Panel is immensely excited about this new direction for the career field, even if that excitement is tempered with apprehension about the hard work necessary to get this new program off the ground. We hope we can count on your help and your counsel as we take cryptanalysis into the next century. See you at the Conference in March!

****

b. ANNOUNCEMENTS

(FSHQ) [redacted] has been named as the new Executive of the CACP. [redacted] has moved out and began her new job in Z409. Her new phone number is [redacted] if you need to get in touch with her.

****

//

5. TECHNICAL HEALTH

a. (FSC) " It Was the SAWUNEH of 94 " by [redacted]

Well another spring and summer has past and we in [redacted] have seen it come and go with the completion of SAWUNEH94. SAWUNEH94, [redacted] Summer Analytical Workshop Up North EH!, has resulted in some good work, very useful programs, some new experiences and a summer program that will hopefully continue on an annual basis for years to come.

[redacted] workshops started back in 1991 when it was decided that one way for CSE to contribute to the crypt effort should be to host workshops that would help focus [redacted] mathematicians on specific problems and would benefit from invited community visitors from NSA and GCHQ.

Well it's 1994 and [redacted] has hosted its fourth SAWUNEH with a very different twist. The workshop started on May 16th and finished on Friday, July 11th. This year, it was [redacted] first time to invite members of academia to participate in the workshop. They were [redacted]

(b)(3)-P.L. 86-36

(b)(6)

(b)(3)-P.L. 86-36

University. Being a bit of a skeptic on how well these academics would perform in our workshop, I really had my doubts that these fellows could stay focused and interested on our workshop problems for eight weeks. Boy, was I surprised! Given the brief introduction to cryptanalysis and cryptomathematics, they still managed to keep a high interest and tremendous amounts of energy to do some outstanding work in the workshop. I tip my hat to them.

The three main topics for SAWUNEH94 were:

Due to the choice of problems and operational requirements, we unfortunately had no- representation from GCHQ, but we received a strong con- tingent from NSA. Our NSA guests included:

(b)(1)
(b)(3)-P.L. 86-36

The topic coordinators for SAWUNEH94 were: for

Being a topic coordinator was not an easy task. Not only were these people involved in doing crypt research on their specific subject, but they were also responsible to put the problem together. This implied collating all the preliminary information such as finding papers, software, and data, and then identifying areas and strategies of research on their pertinent problem. Of course, throughout the workshop, they were keeping the momentum of the research going and seeing things through, chairing regular brainstorming sessions, and, finally, helping in the wrapup of the workshop by writing up a technical report outlining the work performed, results achieved, and new directions of research identified.

(b)(3)-P.L. 86-36

The first official week of SAWUNEH94, which I called "Homecoming Week," consisted of the topic coordinators introducing the problems to be researched and outlining some avenues of investigation. In addition, the invited academics were initiated to cryptanalysis and cryptomathematics, a very grueling exercise for them. But they took it in stride and with a smile on their faces.

Meanwhile, the logistics to set up computer accounts, provide desks and chairs and all the accompanying paraphernalia for working in an office, was interesting to say the least. Because of the presence of the academics, special computer security measures had to be implemented. For the workshop,

The next big headache was setting up accounts so all visitors could sign on easily and have everything set up accordingly, e.g. have good .login and .cshrc files. Thanks to some very computer-wise cryptomathematicians, we were able to set up our visitors so they could log on, send e-mail and do the various EDP tasks as painlessly as possible. It was slow going, but eventually, everything sorted itself out and everyone could get some work done.

Finally, the problem of where to sit all the visitors including the academics was great fun to solve. It was the classic case of musical chairs. For this, a debt of gratitude goes out to the folks who sacrificed their desk to accommo- date the special seating arrangements for the workshop. Special care in deciding where to sit people was needed because we wanted to integrate the academics amongst our mathematicians and our NSA visitors so that everyone could benefit from

(b)(3)-P.L. 86-36

others' experience and knowledge and just simply get to know each other.

Even with moving some people around, we wouldn't be able to accommodate all of the visitors with a desk. So we needed extra office space. A fortuitous situation happened when another office needed to move. When they moved, we simply became squatters and managed to get that room where we could sit four people. A coup d'etat I say! This room became the [redacted] room during the day and the academics' room after hours which enabled them to have a place to continue working on their problems on weekends and such. Being from outside Ottawa, they would often stay late to continue working on some idea or, towards the end of the workshop, finish writing up their reports.

Once all the bugs were worked out at the start of the workshop, serious work began. And what excellent serious work indeed. On the [redacted] problem, we had three academics and our topic coordinator working with an NSA crypto-linguist ([redacted], an NSA cryptanalyst ([redacted]). Together they [redacted] As for [redacted], we had one academic working the problem with our topic coordinator with some valuable assistance from [redacted]. For [redacted], we had a strong contingent of CSE cryptomathematicians working this problem with the help of [redacted]

The results of SAWUNEH94 are that we have produced a good [redacted], some interesting hypotheses on [redacted] From all this work, eight papers were written which have been published and distributed to NSA and GCHQ.

We in [redacted] have found SAWUNEH94 to be a success, even more so with the participation of the academics. It was a first experiment that has provided great dividends. A pat on the back for our mathematicians for a job well done is in order. And many thanks for our NSA visitors whose insights and experience made this SAWUNEH great.

It's now January 1995 and Spring is not too far. Guess what, SAWUNEH95 is coming soon. The dates for SAWUNEH95 will be May 15th to July 14th. The overall workshop coordinator is [redacted]. A list of topics has been sent out to NSA and GCHQ for comments. And if you are one of the few who can come to Ottawa and attend SAWUNEH95, we're looking forward to meeting and working with you.

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

****

b. (~~TOUO~~) Signals Development Conference

1995 Signals Development Symposium

This year's Signals Development Symposium will be held in the Friedman Auditorium from Monday, 3 April through Friday 7, April. The motto for this year's symposium is "Meeting the Challenge", and it will give us an opportunity to review current efforts to analyze and exploit modern communications. Efforts and achievements in the analysis of waveform and bit-level signals will be presented, as well as analytic concepts, systems and tools; a number of demonstrations are planned. Many [redacted] and Second Party activities will be represented. Training will be discussed.

Symposium sessions on digital multiplexers, data networks, HF communications developments, cellular communications, technology issues and software tools are being planned and others may be organized.

This year's Symposium is co-sponsored by Z1, W9S and G2. Arrangements for the conference are being handled by Z15. Please send name of presenter, title and short abstract (~100 words) to [redacted] by February 10, 1995. NOTE: Presentations are limited to a classification level of TOP SECRET CODEWORD. Attendance at the symposium is open to all cleared personnel. The point of contact is [redacted]

(b)(3)-P.L. 86-36

****

//

[redacted]

6. COMMUNITY SERVICE

(b)(3)-P.L. 86-36

a. (U) [redacted] Algorithm and Its Inventor

by

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(FOUO) [redacted] is planning to publish a paper entitled "Some Things I Did in Thirty Years at CCR (and a Few I Did Before)". All cryptanalysts are encouraged to read this paper when it appears, and to learn more about this creative member of our profession.

(b)(3)-P.L. 86-36
(b)(6)

b. (U) Center for Cryptologic History Announcement

Dr. David Kahn has joined the CCH as its 1995 Scholar-in-Residence.

Dr. Kahn has not been cleared and will be undertaking a number of unclassified projects for the CCH. In addition, he will give occasional presentations to special seminars and to NCS classes.

David Kahn
* as a teenager, became interested in cryptology
* A.B., Bucknell University
* Ph.D. in history, Oxford University

* In 1965, published _The Codebreakers_, the first (and most) comprehensive study of how cryptology has affected the course of history
* published _Hitler's Spies_ in 1978
* published _Kahn on Codes_ in 1984
* published _Seizing the ENIGMA_ in 1991
* author of many journal, magazine, and newspaper articles

* has taught at Yale & Columbia Universities
* is a senior editor at the Long Island daily _Newsday_

****

c. (U) February is Math Certification Seminar Month

The math panel will be holding two seminars in February for individuals who are interested in becoming certified as a Cryptologic Mathematician. The Chairman of the Math Career Panel, [redacted] will start the session, and the Exec will present an overview of the certification process; copies of the certification criteria document will be available. Members of the the math panel will explain what they look for when they evaluate a package of papers submitted by an aspirant, and also describe what an individual's supervisor can do to facilitate the process. The remainder of the time will be available for questions and answers. Details about the two seminars are contained in the following two Calendar Appointments (drag-droppable onto Calendar Managers).

(b)(3)-P.L. 86-36

** Calendar Appointment **

[redacted]

Date: 2/21/95
Start: 10:00 am
End: 12:00 pm
What: Math Certification Seminar
Ops 1 - Rm. 2C086

** Calendar Appointment **

Date: 2/24/95
Start: 10:00 am
End: 12:00 pm
What: Math Certification Seminar
S - Rm. C2A57
(DDI Conf. Rm.)

****
//////////

7. Puzzles and Problems

a. (U) Solution to January KRYPTOS puzzle:

"The Light Fantastic" [redacted]

A.	TWINKLE	H.	OUTLIER
B.	POPULAR	I.	CHIMERA
C.	UNKEMPT	J.	CORONET
D.	SMOLDER	K.	BRACKEN
E.	ETERNAL	L.	SKEPTIC
F.	RHOMBUS	M.	ROBOTIC
G.	BETRAYS		

UNCLUED WORD: SUSPECT

R	H	O	M	B	U	S		S		E
O		U		R		U	N	K	E	M	P	T
B	E	T	R	A	Y	S		E		O		E
O		L		C		P	O	P	U	L	A	R
T	W	I	N	K	L	E		T		D		N
I		E		E		C	H	I	M	E	R	A
C	O	R	O	N	E	T		C		R		L

(b)(3)-P.L. 86-36

==========

b. (TSC) Solution to last problem:

November PROBLEM OF THE MONTH by [redacted]

(TSC) The November problem involved the Zendian ambassador's [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

==========

c. (TSC) February PROBLEM OF THE MONTH by [redacted]

(TSC) [redacted] Find as many significant observations as you can, and describe a model that

(b)(3)-P.L. 86-36

[redacted]

will explain as many features as possible. Please e-mail your best model to [redacted]

(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

****
//////////

8. LITERARY/HISTORICAL TIDBIT

a. [redacted]

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

****
//////////

9. ACTION LINE

(U) Question: Why aren't the vote totals of the Kryptos election publicized?

Answer: The simple answer is that, to my knowledge, nobody ever considered doing it. I brought the question before the Kryptos Council which formally decided not to publish election results. Election votes are counted independently by three Council members. The Kryptos Council felt that this process was sufficient to guarantee accuracy and to protect against irregularities. We are very appreciative of those willing to step forward as candidates for positions on the Kryptos Council. Publishing the results could embarrass some of those people while, in our minds, providing no substantive benefit. Perhaps this position seems "undemocratic" and, if there is a ground swell of opinion of Kryptos members against it, we will reconsider. But for now we will continue to publish only the names of the winners.

[redacted]
Kryptos President

(b)(3)-P.L. 86-36

[redacted]

****
//////////

10. EDITORIAL CORNER

If you have a relatively short technical treatise, or anything you would like to have considered for inclusion in future issues, please submit it to any member of the editorial board or any of our office POCs.

PLEASE paragraph classify each item submitted, and USE ASCII FORMAT!

A reminder that anonymity may be requested for Action Line items - in fact, you may mail them in hardcopy form to any member of the editorial board or any of our office representatives.

We would very much like this newsletter to represent a broad cross-section of the CA community - we need some more volunteers to help us, however. Perhaps you would like to work on one of the topics in this issue, or perhaps there is another topic which you think should be included in future issues. Either way, we would like your input, and help, so give one of us a call. The more people who divide up the work, the less burden on any one person.

##########
NOTE: We MUST receive any submissions for the March issue by 23 Feb.
##########

EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum

[redacted] NCS

OFFICE Reps

[redacted]

(b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2, DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR" DATE OF SOURCE: 3 SEP 1991

[redacted]

[redacted]

TOP SECRET//COMINT

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:18
(U)PE EXTERNAL RAGE

****
* TALES OF THE KRYPT *
****
March 1995

##########
//////////

(TSC) TABLE OF CONTENTS:

1. CA Perspective
2. KRYPTOS Society
3. Calendar of Events
4. Word from the CACP
5. Technical Health
6. Community Service
7. Puzzles and Problems
8. Literary/Historical Tidbits
9. Action Line
10. Editorial Corner

##########
//////////

1. (TSC) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of Nicholas Howard, Head of H at GCHQ:

THE CHANGING CHALLENGE OF CRYPTANALYSIS

(U) I am very honored to be the first non-American to be invited to write a lead article for this distinguished publication, which has already established itself as a valuable means whereby the various elements of the crypt community can keep in touch and share ideas.

(S) For as long as I can remember there have been Jeremiahs wandering around the halls of the cryptologic Agencies loaded with doom and gloom: cryptanalysis has had its day, in five years time nothing worthwhile will be readable and the youngsters ought to leave and seek another job while the going's still good. To which I, after 35 years experience both as a working cryptanalyst and as a cryptologic manager, say boldly: "RUBBISH!" How do I dare say that? Why - the evidence is all around us: by common consent 1994 was the best year for UKUSA crypanalysis for a very long time, possibly even since World War II, with significant advances on all the fronts that matter: [redacted] and I can say with pride that the UK made important contributions to all of them.

(b)(3)-P.L. 86-36

(S) In our business two things can be said with certainty:

- The target will continue to get bigger - and more difficult;
- The ability of UKUSA cryptanalysts to deal with enough of it to keep us in business will continue.

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704.

(b)(3)-P.L. 86-36

[redacted]

(TSC) But to do this means that we have to keep up with change, and adapt to new circumstances. One of the biggest challenges in the last few years has been the growth in [redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(C) But in my view [redacted] and indeed I myself have devoted most of my career to it, as I lack the high-powered mathematical abilities needed for [redacted] and the advanced programming skills needed for [redacted]; so it is with great joy that I see [redacted] once again returning to center stage.

[redacted]

(SC) What are the consequences for us of this shift towards more [redacted] Above all, we need a very special kind of analyst, one with three eyes, which stand for Inspiration, Intuition and Imagination. Formal qualifications are not a prerequisite for these attributes, but even so such analysts are harder to find than professional mathematicians or programmers, and indeed are rarer on the ground in general! They also need a working medium where they can exchange ideas, hypotheses etc. without risk that anyone will denounce them as silly (I hesitate to think how many silly ideas have turned out to be right!). For this reason the close UKUSA cooperation in crypt, which has stood us all in such good stead over the last 50 years and more, becomes ever more important still; analysts at each Agency can bounce ideas off each other, and the friendly cooperation (which at times can almost look like rivalry) between us ensures that we take each other's ideas seriously. Intractable though the old [redacted] problems generally were, the spirit of co-operation between [redacted] was second to none, as many old hands in both will readily testify.

(b)(3)-P.L. 86-36

(C) A key element in the UKUSA crypt cooperation is the integree exchange program. Someone - it may well have been Winston Churchill - once said that the British and the Americans were two nations divided by a common language; but the differences between us (which of course exist between any pair of nations, even the English and the Scots who have been politically united for nearly 300 years) are not fully appreciated until one has had the chance to live and work in the other country and make the most of the best aspects of both. For this reason both of our Agencies see the integree exchange program as so important an element in securing the future health of the relationship that it has always been policy at both Agencies (all Agencies, I should say, because CSE and DSD have long participated in the integree exchange program, and this year sees GCHQ's first integree from GCSB (Government Communications Security Bureau in New Zealand) only to exchange

[redacted]

analysts with proven track records as integrees. For myself, I unquestionably did the best work of my entire career during my three years at NSA (in [redacted] of course!) in 1967-70.

(U) So may I end by inviting you all to think hard about putting your name forward for consideration as an integree; it'll be the best investment you ever made for your future, and for the future of our profession.

//

2. KRYPTOS SOCIETY

(U) In conjunction with CMI, KRYPTOS sponsored a Mardi Gras celebration, at the Last Chance Saloon in Columbia, on 28 February. Over 80 people attended and thoroughly enjoyed mingling and munching! There were plenty of hors d'oeurves and liquid refreshments, and a great time was had by all! Put Mardi Gras on your calendars for next year too, and we'll see about doing it again! Special thanks to [redacted] and her committee: [redacted]

(b)(3)-P.L. 86-36

//

3. ~~(TS//SI)~~ CALENDAR OF EVENTS

March 3	CLA Talk: "Islamic Encounters with Modernity: The Social Dimensions of Islam in Comtempory Indonesia" (9A135 1300)
March 9	CMI Talk: "Quantum Computing: How to do Exponential Work in Linear Time and Space" [redacted] (Friedman, 0930)
March 13	KRYPTOS Talk - "Examples of CA Support to [redacted] (Friedman, 1300)
March 14	Tech Track and the Application Process - Panel of Z TTRP Chairs/Reps (9A135, 1300-1500)
March 14	NSA Science and Engineering Society Talk - [redacted] ADO DEFSMAC, addressing DEFSMAC's role and mission, including their role in [redacted]
March 15	G21 Telecommunications Technology Forum
March 16	GNI Day Sponsored by K06 - Demos and Briefings from Across the Agency - (R&E Symposium Center, 0815-1530)
March 16	CLA/IAI Talk: "Contemporary American Foreign Policy", [redacted] Balt. Council Foreign Policy (9A135 1300)
March 16-19	3rd International Conference on Telecommunication Systems Modelling and Analysis (Nashville, Tenn.; (615) 322-3694
March 22	Talk on "Mathematics Education Reform" [redacted] Dartmouth (Friedman, 0900)
March 22-24	CISS `95, Conference on Information Sciences and Systems; (John Hopkins University; Baltimore, MD; (410 516-7031)
March 27-31	CARD (GCHQ)

(b)(1)
(b)(3)-P.L. 86-36

(b)(6)

(b)(3)-P.L. 86-36

[redacted]

March 28-31	IPCCC `95, Annual IEEE International Phoenix Conference on Computers and Communications; (Arizona State University; Phoenix, AZ; 602-965-7775)
March 29-30	1995 Cryptanalysis Conference (SRC)

PLAN AHEAD -

April 3-7	1995 Signals Development Symposium (Friedman Auditorium)
May 1-5	ACE (CCR Princeton)
May 3	CLA Speaker "Language Policies in the United States" (OPS2B 4118, #6, 1300)
May 23-25	CA PQE
June 1	CMI Banquet (BBC, 1830-2300)
June 1	MATHFEST 95
June 5-9	CA-305

//

4. CACP NEWS

a. (~~FOUO~~) Changes

[redacted] has been named a Member of the CACP.

[redacted] has replaced [redacted] on the Technical Paper Evaluation Board.

[redacted] will replace [redacted] on the Technical Paper Evaluation Board.

(b)(3)-P.L. 86-36

b. (~~FOUO~~) CA Conference Update

Invitations have been sent out for the 1995 CA Conference: CA 2000. The conference will focus on the development of the new certification requirements for a professional cryptanalyst. Individuals who did not receive an invitation but who would like to express their thoughts or concerns regarding the new certification requirements should speak with a Panel member before the conference.

//

5. TECHNICAL HEALTH

a. (~~FOUO~~) CRYPTOLOGIC QUARTERLY NEEDS ARTICLES!

(~~FOUO~~) Cryptologic Quarterly is looking for a few, actually many, good articles. If you have recently written a paper or report (other than SIGINT product) on a cryptologic topic, whether it be a professionalization paper, a technical report, paper for an NCS class, or anything else you think might be of interest to the cryptologic work force, please get in touch with us. Articles written just for the Quarterly are, of course, always sought. To give you an idea of the kinds of contributions we're looking for, here's what our editorial policy, as stated on the CQ's title page, says:

"The goal of Cryptologic Quarterly is to educate the work force in both the narrow technical elements of the cryptologic effort and the broad issues that affect that effort. Articles for Cryptologic Quarterly may be written on any theoretical, doctrinal, operational, managerial, or historical aspect of cryptology. The criterion for publication is whether or

(b)(3)-P.L. 86-36

[redacted]

not the article is of sufficient substance and interest to make a genuine contribution to cryptologic literature."

~~(S-CCO)~~ And to give you an idea of the various subjects CQ authors write about, here are the articles that appeared in the Fall 1994 issue:

Old BOURBON--1947: The Third Year of Allied Collaborative COMINT Effort against the Soviet Union ~~(S-CCO)~~

The Collection Challenges Represented by the [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

The Cryptographic Mathematics of Enigma (U)

[redacted]

Project [redacted] (U)

(b)(3)-P.L. 86-36

Signaling System No. 7: And What about Analysis (U)

Code Acquisition by Binary Autodirective Search (U)

~~(FOUO)~~ If you have something you've already written and think it might be a candidate for publication in Cryptologic Quarterly, or if you have any questions about writing such an article, please call Barry Carleen, Executive Editor, at [redacted]

~~(FOUO)~~ The Quarterly is NSA's professional journal, and it needs contributions from professionals if it is to accomplish its goals. We know you potential authors are out there--and we would like to hear from you.

//

6. COMMUNITY SERVICE

a. ~~(FOUO)~~

A LOOK AT THE MATHEMATICS EDUCATION REFORM EFFORT:

WHAT IS GOING ON?

[redacted]

Dartmouth College

(b)(6)

9:00 a.m., Wednesday, 22 March 1994
Friedman Auditorium

This Talk Is Unclassified

Throughout the 80s national attention has been drawn to perceived problems with mathematics education in the US. NCTM has responded with its "Standards", the Council of Governors under George Bush set goals for improvement by the year 2000, and calculus reform efforts have extended the effort into the colleges and universities.

What, in fact, are the problems? Are they real? What changes are actually taking place in the colleges and universities? Apart from changes in the way mathematics is being taught, what does the reform effort actually have to say about mathematics itself? What, in short, is the "beef"?

The talk will survey some of the background and will report on what mathematics departments are doing. It will contain specific examples

(b)(3)-P.L. 86-36

[redacted]

drawn from some of the reform efforts of departments.

[redacted] is the immediate past president of the Mathematical Association of America and a leading proponent of mathematics education reform. His presentation should be of interest to anyone who uses mathematics or has a student in a math course. (b) (6)

For more information, contact: [redacted]

****

b. ~~(C-CCO)~~ COMMUNICATIONS RESEARCH E-MAIL
What is it and why might you care?
(Submitted by [redacted])

CRE is basically an E-mail bulletin board which connects people all over the Agency who have an interest in communications research or related topics. There are often queries regarding telecommunications in general or about uses by a specific target. You can ask questions, provide answers, or simply absorb information. This 'topic' is not available via Enlighten because not all of the interested parties have access to that forum. Participation is open to all TS/SI cleared GREEN BADGE (NSA) AND GOLD BADGE (U.S. Military and 2nd Party) analysts (i.e., not BLACK BADGE contractors or consultants). (b)(3)-P.L. 86-36

To register for the CRE, send E-mail to the moderato [redacted]
Include:

- Your NAME, Organization, building/room *, secure phone
  (* personnel outside CONUS give "site" vice "building/room")
- Your E-mail address as SID@NSA
- Your BADGE Color (GREEN or GOLD, not BLACK)
  If not GREEN, also give nationality

That's it. The moderator will add you to the CRE distribution list and you will begin to receive CRE-mail. Soon thereafter the moderator will send you a copy of the guidelines and a recap of recent messages.

Submissions may be on any WORK-RELATED subject pertaining to Communications Research. Each message need not appeal to all participants.

The format of CRE is informal. There is a moderator but he does not filter submissions. Whatever you send to the CRE is automatically sent verbatim to ALL CRE subscribers, though you may of course respond to someone's query directly without sending your response arn something!

Try it. You might like it!

If you have questions, contact [redacted] (b)(3)-P.L. 86-36

****

c. (U) ARCHIVAL EXHIBITS

1. Shootdown of Admiral Yamamoto - On Exhibit in the NSA Records Center

2. Native American Code Talkers - Available for display. The National Cryptologic Museum has been given a copy of this exhibit which it intends to keep on permanent display. Future displays of this exhibit will be outside the Friedman Auditorium in April for a special ceremony honoring Choctaw and Comanche code talkers.

3. Capture of U-505 - Nimitz Library, U.S. Naval Academy

4. Deception at D-Day - National Defense University,

(b)(3)-P.L. 86-36

[redacted]

Washington D.C.

//

7. (U) PUZZLE (Send your solution to our Puzzle Editor, [redacted] and we will publish the names of all those who solved this one.)

(b)(3)-P.L. 86-36

B-Gone!

In this puzzle the letters A-Z are assigned the values 1-26 in that order, and are placed in the 5x5 diagram below. The number in a cell has nothing to do with the letter which belongs in that cell, but rather is the sum of the values in the cells immediately adjacent horizontally and vertically.

Example: 48 is the sum of T(20), H(8), P(16) and D(4).

	H	
T	48	P
	D	

In this puzzle, the letter "B" has been omitted, and the letter "O" has been placed in the center cell for you. When the diagram is completed, no two letters that are consecutive in the alphabet will be in the same column, row or diagonal with one other. For the purposes of this puzzle, the letters Z and A are considered to be consecutive, as are A and C (since "B" is omitted).

37	53	42	33	23
29	61	63	62	25
41	60	O 54	61	41
44	31	87	53	54
16	65	29	59	23

//

8. TIDBITS (Compiled by [redacted]) (b)(3)-P.L. 86-36

a. (U) Dedication of the William F. and Elizebeth S. Friedman Auditorium

On 27 October 1994, the "Friedman" Auditorium was in fact rededicated, this time to reflect the fact that many consider Elizebeth Friedman to have been fully equal in talent and accomplishments to her better-known husband.

Partners for Life - At Home and At Work

In 1623 Sir Francis Bacon created his "biliteral alphabet", which used only combinations of the letters "a" and "b" to represent the entire alphabet. In his table, "aaaaa" stood for "A", "aaaab" for "B", "aaaba" for "C", etc. He suggested it could be hidden in ordinary text by using two different typefaces. William and Elizebeth Friedman represent a "biliteral" approach to the study of the art and science of cryptology. They met at Riverbank Laboratories, in Geneva, Illinois, near Chicago. (This was the creation of the eccentric millionaire

(b)(3)-P.L. 86-36

[redacted]

George Fabyan, who enlisted people to explore a variety of subjects in his laboratories, from plant genetics to cryptology. Elizebeth was hired to help prove that Sir Francis Bacon wrote Shakespeare's plays and sonnets.)

After spending the winter of 1916-17 studying everything they could find on secret writings (American sources included a couple of short works by military men, and two articles and a story by Edgar Allen Poe), William and Elizebeth decided to marry and spend their private, as well as their professional, lives together.

This combination of a genetics major and an English major provided the basis for the science of modern American cryptology. Until the creation of the Army's Cipher Bureau in 1917, the team at Riverbank was the only organization in the country capable of solving secret messages. After 1917 the Friedmans stayed involved in the training of Army officers until William joined the Army and spent time in France studying German code books with the American Expeditionary Force. Early in 1921 the two were offered six-month trial employment as civilian "code experts" for the Army in Washington, D.C.

While William was solving the Hebern machine and other ciphers for the War Department, Elizebeth was on loan as a "special agent" to the Customs Department from the Department of Justice. During a three-year period, she and her assistants solved 12,000 encoded and enciphered radio messages from rumrunners seeking to circumvent the Prohibition Act. In 1934, due to her testimony from decrypted telegraph messages, a major diplomatic incident between Canada and the U.S. was resolved. (A Canadian-flagged schooner had been chased down and sunk by the Coast Guard when suspected of illegal activities. The owner actually proved to be involved in a New York smuggling ring.) In 1937 Elizebeth was asked by the Canadian government to testify against opium dealers working in the Vancouver area. (She had solved their complicated code without knowing Chinese.)

During World War II, while William was busy trying to solve the Red and Purple Japanese cipher machines, Elizebeth was also busy supporting the U.S. war effort. She devised a code system for the Office of Strategic Services (OSS), and solved cipher messages sent by German spies in Allied lands. In 1944 she helped solve the Doll Woman case, where an antique doll dealer in New York was spying for the Japanese. (A letter containing coded information was a source of suspicion.)

After the war William was a cryptanalyst for the predecessor agencies and, finally, the present National Security Agency. Elizebeth worked as a consultant for the International Monetary Fund, setting up a secure communications system.

Both Friedmans returned to the project which had initially brought them together - the Shakespeare problem. Their book, "The Shakespearean Ciphers Examined", is considered the definitive work on the subject, disproving all claims that Bacon wrote the plays.

(Information for this article was extracted from notes used in the rededication of the Friedman Auditorium to the Elizebeth and William Friedman Auditorium, and The Friedman Legacy: A Tribute to William and Elizebeth Friedman, Sources in Cryptologic History Number 3.)

****

b. (U) Callimahos Flutes Shown at Mid-Atlantic Flute Fair

On Sunday, 26 February, at the Holiday Inn in College Park, the Mid-Atlantic Flute Fair was the venue for the display of several items belonging to or pertaining to Lambros Callimahos, reknowned guru of cryptanalysis, cryptologist and flautist. Andrew Callimahos, son of Lambros, and a flautist in his own right, and Helen Callimahos Hurry, wife of Lambros, were both there to talk to interested persons. Andrew recalled wanting to learn to play an instrument when he was nine, and being steered away from double-bass to flute by his father. Helen recalled several events in the life of Lambros. Lambros was born in Egypt of a Greek newspaper editor and a schoolteacher, and moved to New

York when a young boy. He became involved in the Boy Scouts and played fife in the Boy Scout band when he was sixteen. He realized the potential of the instrument and went on to play the first ever all flute concert in Carnegie Hall. The specially-designed flute with which he played was later stolen. The company which designed it, however, got a call nine years later from a pawn shop in New York, describing an unusual flute (it has several extra keys) which they recognized as the one they had designed for Lambros! At twenty-six he was the youngest flute instructor in Salzburg, Austria.

Through the Army, during the war, he entered the field of cryptology, and he and his wife were good friends of the Friedmans. Helen now lives in New Jersey in the small town where both she and Lambros were raised. She keeps active as a docent for the Victorian-style Centennial House across the street from her home.

****
//////////

9. ACTION LINE

It appears as if everyone is happy, and totally informed about everything, as we have had no questions submitted recently! A reminder that we will, if requested, keep the name of the questioner anonymous.

//////////

10. EDITORIAL CORNER

If you have a relatively short technical treatise, or anything you would like to have considered for inclusion in future issues, please submit it to any member of the editorial board or any of our office POCs.

PLEASE paragraph classify each item submitted, and USE ASCII FORMAT!

A reminder that anonymity may be requested for Action Line items - in fact, you may mail them in hardcopy form to any member of the editorial board or any of our office representatives.

We would very much like this newsletter to represent a broad cross-section of the CA community - we need some more volunteers to help us, however. Perhaps you would like to work on one of the topics in this issue, or perhaps there is another topic which you think should be included in future issues. Either way, we would like your input, and help, so give one of us a call. The more people who divide up the work, the less burden on any one person.

##########
NOTE: We MUST receive any submissions for the April issue by 24 March.
##########

EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum

[redacted] NCS

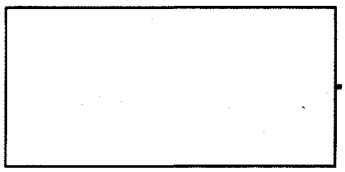
OFFICE Reps

Z03
Z09
Z1
Z2

[redacted]

(b)(3)-P.L. 86-36

[redacted]



(b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

[redacted]

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:17
(U)PE EXTERNAL PAGE

(b)(3)-P.L. 86-36

****
* TALES OF THE KRYPT *
****
April 1995

##
//

(TSCG) TABLE OF CONTENTS:

1. CA Perspective

2. Calendar of Events

3. Word from the CACP

4. Community Service

5. Technical Health

6. Literary/Historical Tidbits

7. Action Line

8. Editorial Corner

##
//

1. (TSC) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of [redacted] Chief Z4.

(b)(3)-P.L. 86-36

Our Future -- Penetrating Secure, Pervasive Cryptography

(TSC) Cryptography, which was a national security and military technology, is rapidly becoming a dual-use technology. As Tom Lessard pointed out in the first of this series, secure cryptography is likely to permeate the environment we see in the future. Many of the [redacted] The common carriers are starting to encrypt such signals as telephone dialing, cellular phones and much more. INFOSEC, formerly a national security requirement, has become a commercial requirement. Law firms would use the Internet if they thought their e-mails about their clients' cases would be safe from prying eyes. I would use the Internet to purchase goods if I thought my credit card number would be safe from theft. Networking and on-line computer records have provided alluring targets for a new breed of criminal. Cryptography is a means of protecting the privacy, integrity and authenticity of data on a network. The cryptographic algorithms used are likely to be well-thought-out. Fortunately for us, as

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # {61704

[redacted] (b)(3)-P.L. 86-36

cryptanalysts (and less fortunately for us as users of the electronic highway and purchasers of security software), the total cryptographic system, including key management, distribution, training, etc. is much less likely to have been given the same degree of care. Anyone who has dealt with cryptographers in the open community such as [redacted] knows that they are the peers of our best in every manner except one: they do not have our experience in looking at the wonderful variety of targets we have faced and have not seen the subtle mistakes these adversaries have made.

(b)(6)

Keys to our Future -- People and Teamwork and Learning

~~(TSC)~~ Continuing to succeed against this formidable challenge will mean we must leverage every advantage we have. The keys to our future are people, teamwork, learning and planning. We must foster excellence in our people and ensure they have the opportunities to develop the skills needed to succeed in attacking this cryptography. Team work is essential, not only within the CA community, but within NSA, with industry, other government agencies and our foreign partners. We must do a much better job of planning. We need to adopt a more business-like outlook. We must know where our "profit" comes from, where our weaknesses and strengths are. We then need to plan to penetrate the technologies or targets that are most likely to satisfy our requirements.

Technical Excellence, Team Work and Strategic Alliances

~~(TSC)~~ We must maintain our technical excellence, but maintaining it means changing and developing. Currently we are being challenged by telecommunications technology changing at a faster rate than ever. As, I believe, the Mad Hatter said, "You must run as fast as you can just to stay in one place." [redacted] One experience I cherish in my career is my time in the [redacted] program, largely because I saw cryptanalysts cooperate with engineers and [redacted] all from different organizations or agencies. Our future success depends on leveraging the talents of people from at least as wide a variety of places and skills. Part of this team work will be forming strategic alliances. GCHQ is a model of a strategic alliance that we have had for years, but this alliance was based on the alliance between our two countries to face a common threat. We have lately seen industry form strategic alliances with competitors, e.g., IBM and Apple to develop the Power PC chip. I believe many of our alliances in the future are likely to be similar, limited alliances on limited topics with organizations that are our competition in other ways. These are much more difficult to manage but are likely to dominate. Some examples of these are DO and ISSO, NSA and Second Parties, and NSA and other government agencies, but most of all we need [redacted] There are few other organizations these days with exactly the same aims as ours, so alliances will usually be uncomfortable, but the difficulty of the challenges makes alliances essential. We cannot succeed on our own technical prowess alone; we must stand on the shoulders of others to see where we must go. Alliances can provide the shoulder. In order to participate in these alliances, to judge which ones are productive and just to attract first class partners, we must be first class ourselves.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

Business Outlook

(FOUO) In the past three years, we have been under increasing demand, primarily from Congress, to justify our budget, people and output in a comprehensible manner. They are doing us a favor. In order to face the challenges of the future, we need to know what our most and least "profitable" efforts are. We need to be much quicker to cut our losses on projects. We have a tendency to declare everything a winner. We need to start more projects and kill more projects. We need to know how much effort we are expending on various problems. This must extend to the development we do, not just the exploitation. Most people in Z are primarily developing new products not producing old products. Even in [redacted] the organizations that have the most people involved in exploitation, many people are developing new products, not maintaining the production of old ones. Since most people are involved in development, we need to know how we are spending that effort and how effective it is. Measuring development is difficult to do; it may be hard to explain your rationale to outsiders, but most of our effort is spent in development, and we need to manage it in a more quantitative manner than we have up to now.

Conclusion --

(U) I find it a little embarrassing to admit that I like the nineties. I like knowing we are facing up to harder challenges than ever before, that we are squeezing more from the taxpayers' dollars. I have always been proud to work at NSA and lucky to have spent most of my time in the cryptanalytic/cryptographic community with people who are collectively, according to Washingtonian Magazine, "One of the smartest people in Washington."

//

2. (FOUO) CALENDAR OF EVENTS

April 3-7	1995 Signals Development Symposium (Friedman Auditorium)
April 18	NSA Science & Engineering Society Talk - Dr. Peter Runge, "Future Directions of Undersea Fiber Optic Communications Systems" (R&E Symposium Center, 1000) (see 4b)
April 19-20	3rd Annual Multimedia EXPO (N. Cafeteria, Special Activities Room)

(b)(3)-P.L. 86-36

PLAN AHEAD -

May 1-5	ACE (CCR Princeton)
May 8	Z Technology Forum; "An Inside Look at the [redacted] (FOUO)"; by [redacted] 1300-1400, OPS2B 4118 Rm.6.
May 3	CLA Speaker "Language Policies in the United States" (OPS2B 4118, #6, 1300)

[redacted] (b)(3)-P.L. 86-36

May 15	Seminar on "Bent and Other Highly Non-Linear Boolean Functions" (see 4a)
May 23	Crypto-Linguistic Association Banquet (Ft. Meade Officers' Club, 1130-1330)
May 23-25	CA PQE
June 1	CMI Banquet (BBC, 1830-2300)
June 1	MATHFEST 95
June 5-9	CA-305

****
//////////

3. WORD FROM THE CACP

a. (C) Third Annual Cryptanalysis Conference - "CA 2000"

The third annual Cryptanalysis Conference, held on 29 and 30 March at the Supercomputing Research Center in Bowie, was a resounding success. Nearly 90 people participated, and those attending included both certified cryptanalysts and professionals in the other disciplines involved in cryptanalysis. The focus of this conference was to discuss new criteria for certification in CA that will help our career field to prepare to enter the 21st century.

Changing resources (downsizing), changing world situations, and technological advances require today's cryppies to do many things that our current professionalization criteria do not address. The CA Career Panel did quite a bit of research and brainstorming during the latter half of 1994 to devise new, more relevant criteria, and armed with a sketchy proposal, invited members of the community as well as experts from related fields (or "integral disciplines") to pick it apart, fill in the gaps, and offer suggestions about what a professional cryptanalyst needs to know and be able to do now and in the future. You may have read about some of these proposed changes in the February issue of "Tales of the Krypt", or heard about them via word of mouth.

After some preliminary speeches, the conference attendees broke into seven working groups to focus on various aspects of the proposal, along with other issues. Some were tasked with identifying areas of knowledge that all cryptanalysts should have, as well as which areas should be suggested but optional; others were tasked with doing some preliminary course development, and still others with providing a "sanity check" for the whole process.

All groups worked very hard to come up with fair and useful recommendations for the Panel. A presentation was made by each working group on the afternoon of the second day, and a more detailed, written report will eventually be submitted by each group. We hope to publish a conference report containing both the recommendations of all the working groups and the speeches made to the entire body in early May.

One concern that was expressed by many involved our plans to do away with the PQE. Several alternatives were suggested, and in light of the fact that the Career Panel still has much work to do on the new criteria, it is likely that the PQE will be around for a long time, in one form or another. So if you were holding off on taking the exam

because you thought it might be replaced by coursework, rush right over to the CA panel office and sign up for the May offering!

---

b. (~~FOUO~~) Sign-up for the CAPQE, which will be held on May 23, 24 and 25, is underway in the CA Career Panel Office. Aspirants are encouraged to contact the Panel office if they are unsure of their eligibility. Below is a schedule of the CAPQE review sessions.

1995 CAPQE REVIEW SESSIONS:

SESSION I: CA110 REVIEW - [redacted]
03 April, 1100 - 1300, 3C082
04 April, 1000 - 1200, 3C082

SESSION II: CA123 REVIEW - [redacted]
05 April, 1100 - 1300, 3C082
06 April, 1100 - 1300, 3C082

SESSION III: MACHINE CA REVIEW - [redacted]
10 April, 1000 - 1130, 3C086
11 April, 1200 - 1400, 3W083
12 April, 1100 - 1300, 3C082
13 April, 1000 - 1200, 3C082
14 April, 1100 - 1300, 3C082

SESSION IV: ESSAY REVIEW - [redacted]
19 April, 1100 - 1300, 3C082

SESSION V: MANUAL CA REVIEW - [redacted]
24 April, 1100 - 1300, 3C082
25 April, 1100 - 1300, 3C082
26 April, 1100 - 1300, 3C082
27 April, 1100 - 1300, 3C082
28 April, 1100 - 1300, 3C082

(b)(3)-P.L. 86-36

---

c. (~~FOUO~~) The CACP will hold a Technical Track Titling Ceremony on 11 April 1995, at 1400 hours, in 9A135. Refreshments will follow. Please call the Panel office for a reservation.

---

d. (~~FOUO~~) Announcements

[redacted] has been named as the newest CACP Member. He has replaced [redacted]

[redacted], has replaced [redacted] and [redacted] has replaced [redacted] on the Computer Program Evaluation Board (CPEB).

[redacted] is the newest member of the CA Technical Track Review Panel (TTRP).

Graduating CA interns [redacted] will be joining [redacted] for their permanent assignments.

The Cryptanalysis Career Panel presented [redacted] with a cash award for the honors computer program he submitted for CA

(b)(3)-P.L. 86-36

[redacted]

certification. Occasionally a technical paper or computer program submitted for CA certification is of such a caliber that it not only passes, but passes "with honors," as John's did. We congratulate John on his fine work and wish him continued success.

****
//////////

4. COMMUNITY SERVICE

a. ~~(FOUO)~~ Upcoming Cryptologic Mathematics Seminar (see calendar)

[redacted] a distinguished researcher in cryptologic mathematics, will present a one-day seminar at the Agency May 15. [redacted] has published several scholarly papers on bent functions and their application to cryptography. The title of her seminar will be "Bent and Other Highly Nonlinear Boolean Functions." (b) (6)

Details of her visit will be announced later. Mark your calendars and plan to hear a leading practitioner of theoretical cryptomathematics discuss topics of considerable interest to Agency professionals. Questions may be addressed to [redacted] (b) (3)-P.L. 86-36

****

b. ~~(FOUO)~~ NSA Science and Engineering Presentation (see calendar)

The NSA Science and Engineering Society will sponsor a presentation by [redacted] the Director of the Undersea Lightwave System Implementation Division at AT&T Bell Laboratories. [redacted] a pioneer in fiber optic technology, holds MS and Ph.D. degrees from the Technical University of Braunschweig, Germany. He has been honored with prestigious awards from the Optical Society of America and the Institute of Electrical and Electronic Engineers. He is currently responsible for undersea fiber optic cable installation, testing, maintenance and integration and for specifying future systems. The title of [redacted] talk is - (b) (6)

"Future Directions of Undersea Fiber Optic Communications Systems."

****

c. (U) CLA 30th Annual Banquet

The Crypto-Linguistic Association is very fortunate to have for our guest speakers this year [redacted] and [redacted] curators of Marine Mammals at the National Aquarium in Baltimore. They will be speaking about "How Dolphins and Seals Communicate." Their presentation will include dolphin and seal "communications" and videos. Come and see how "aliens" on our own planet communicate!

In addition, the winners of the 1995 Jaffe, Rochefort, and [redacted] Awards will be announced at the banquet. Come celebrate 30 years of fellowship and linguistic adventure and excellence!

Tickets will be on sale until 12 May, and may be obtained from - (b) (3)-P.L. 86-36

[redacted]

[redacted]

[redacted] (b)(3)-P.L. 86-36

d. ~~(S-CCO)~~ CRYPTOLOGIC ALMANAC: NSA's First NSOC

~~(S-CCO)~~ At the time the Armed Forces Security Agency (AFSA) was reorganized into NSA in 1952, the AFSA Watch Office was staffed by two officers and a group of enlisted personnel, arranged into four shifts. The office was under the Production organization, and its functions were the same as some of NSOC's today: personnel scanned traffic and would call in analysts to handle problems; they also disseminated items of special interest to customers. Eventually, they were tasked with giving a daily intelligence briefing. While various proposals were made to place the Watch Office on the Director's staff and endow it with the authority to make after-hours decisions, none were adopted.

~~(S)~~ By 1958 the Watch Office had seventeen people, split between military and civilians. When the CRITIC program was established that year, the Watch Office was made responsible for monitoring NSA CRITIC handling, including placing proper addressees on CRITIC messages.

~~(S-CCO)~~ A temporary command post was set up at NSA in response to the Cuban Missile Crisis in 1962. Its senior officer was authorized to act for the Assistant Director for Production during nonduty hours. This led to the Interim Command Center in January 1963. Staffed at forty to fifty personnel, the ICC also produced several summaries and watch reports.

~~(S-CCO)~~ A permanent NSA Command Center was established on 1 March 1963, once again subordinated to the Production organization; personnel came from each of the Groups. Central Reference provided one assignee. Additional duties included producing the SIGINT Daily Summary.

~~(S-CCO)~~ Other NSA organizations also had established watch operations-- in fact, other elements in Production established watch teams of analysts-- in response to worldwide crises including the North Korean capture of the PUEBLO and the Tet Offensive in Vietnam in 1968. After the PUEBLO incident, and especially after the shootdown of the EC-121 aircraft in 1969, the need to consolidate Agency watch operations and to have someone available during nonduty hours to speak for the Director became apparent, and the then-Assistant Director for production, Major General John Morrison, USAF, worked to bring the disparate elements together into what we know today as the National SIGINT Operations Center (NSOC).

[David A. Hatch, Director, Center for Cryptologic History, [redacted]
or [redacted] (b)(3)-P.L. 86-36

//

[redacted]

5. (S) TECHNICAL HEALTH

Painting a Room - Cryptanalysis from a Different Perspective (U)
by [redacted] (b)(3)-P.L. 86-36

(U) While painting an upstairs bedroom one weekend, I realized the process was similar to the cryptanalysis of a new system.

Step 1 -- Preparation (U)

(U) Have you ever noticed how it seems to take longer to prepare a room for painting than to do the actual painting itself? I carefully removed the contents of the bedroom to another room, sorting into two piles the things to be saved and the things to go to Help Laurel or Amvets.

[redacted]

(U) The next step was to clean the area to be painted -- the walls, floors, etc. Taking my stack of saved newspapers, I spread them over the floor, covered the whole with a plastic dropcloth, and used masking tape to cover the molding around the edge of the rooms.

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Step 2 -- Diagnosis (U)

(U) Now I was ready to begin painting. Oops! I forgot to collect the tools to use -- the paintbrush, sponge edger, large and small rollers, and most important, the paint. Being a conservationist at heart, I took the one full and one partial can of paint left from painting two previous rooms and mixed the two together -- one light aqua and one-half pale pink did not make the expected lavender, but a shade lighter aqua -- oh, well!

[redacted]

Step 3 -- Solution (U)

(U) Bringing in the team for the actual work, my youngest daughter and I began painting, she using the small roller, and I the large.

[redacted]

(U) Uh-oh, I neglected to tape the top edge of the white baseboard. Well, I planned to paint that white again anyway.

(U) Small diversions from the straight and narrow track of diagnosis/hypothesis/solution can often be corrected by later analysis.

(b)(3)-P.L. 86-36

[redacted]

(U) My daughter gave up early, while I plugged along trying to finish the initial coverage of the walls. The trim would wait for another day. I brought in lamps as our natural sunlight failed to illuminate the room.

(S) Additional people with new ideas

(U) I turned to a paintbrush and edger for the top of the wall where it meets the ceiling and discovered I had neglected to bring the ladder up from the basement.

(U) Frustration set in as I scurried to finish late in the evening, and my paintbrush slipped now and then with a swoop of blue against the white of the ceiling.

(U) I cleaned up the tools for the night and prepared to go to bed.

(U) Sometimes a break is needed from analysis of a cryptosystem as well, so we can get "a fresh start in the morning."

(U) The next day I surveyed the results of my work of the night before, seeking my husband's opinion on whether a second coat of paint would be necessary. Considering the slight greenish cast to one wall would be covered by a bookcase, I decided to proceed to the painting of the trim.

(U) Again I had to prepare for the painting of the trim by cleaning the window sills and taping around the edges.

(U) Using a paintbrush I finished up the trim work, touching up places on the ceiling I had accidentally painted blue and covering over the blue spots on the baseboard.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

a bookcase."

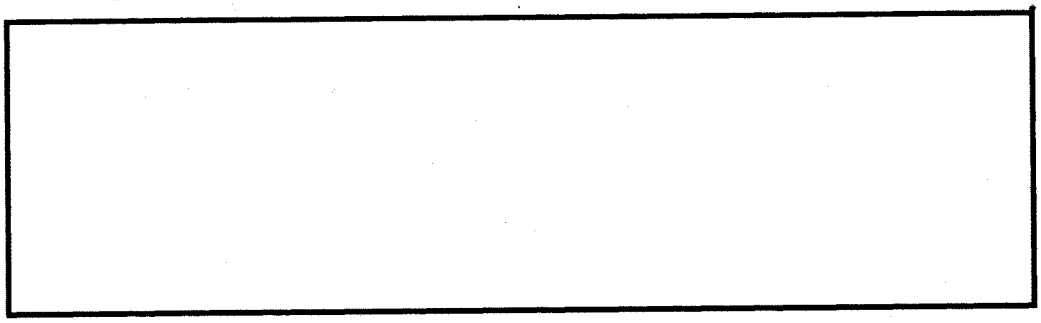
(U) Now to the final cleanup -- all the tools were washed up and put away for the next time; the drop cloth and newspapers were cleared away and disposed of.

(U) Programs are labeled, and copies of early test results and worksheets deleted or thrown away.

Step 4 -- Exploitation

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) The furnishings were moved back into the room; the newly-washed curtains rehung. Yea! It's finished and it looks beautiful!



(U) Now, it is time to sit back, relax and enjoy the refreshing atmosphere of a "new room", and the satisfying feeling of a finished job!

****
//////////

6. (U) LITERARY/HISTORICAL TIDBITS

a. (U) THE CRYPT BUG (by MASTER SGT. Charles Murray)

When all good folks are sound asleep,
And all the rest are counting sheep,
He concentrates on cipher text,
And contemplates ways most complex
To render an approved solution
Of some obscure substitution.

While all the world is sleeping, snoring
Loud enough to rip the flooring,
He derives much satisfaction
>From the spatial interaction
Of poly-graphic frequencies
And isomorphic sequences,
Of characters on paper slips
Better known as sliding strips.

Slides them West and tries the "Chi" test,
Slides them East and tries the "Phi" text,
Clamps his pipe tight in his mouth,
And grimly slides them North and South,
And if success eludes him then,
Tears them up and starts again.
Meanwhile the clock ticks on and on,
Until at long last comes the dawn.

As the milkman rattles by,
He is heard to heave a sigh,
Slowly piles the work sheets higher,
Calmly throws them on the fire,
Having proved one simple fact;
There can be no doubt of that-
As suspected all along,
Everything he did was wrong.

Reprinted from The Signal Corps Bulletin. July-December 1940 - 109.
War Department, Office of the Chief Signal Officer. Washington DC.

b. ~~(C)~~ A CRYPTANALYST'S ENCOUNTER WITH ROYALTY (by [redacted] (b)(3)-P.L. 86-36

(U) Here is the real scoop, right from the notorious cryppie herself!

~~(TSCUO)~~ I wasn't too tightly wrapped. Honestly, I believe the Americans in the GCHQ community were even more excited about the visit of Queen Elizabeth and Prince Philip than the British! (b)(1) (b)(3)-P.L. 86-36

~~(C)~~ Now, our office is next door to one the royals visited. (The [redacted] I think, which controls [redacted] The royal entourage went in [redacted] back door for a briefing, rather than wind throu the hallways. OUR back (fire) door is right nearby so of course we were all hanging out. It was great, and when we went back inside, someone said 'oh, when the Prince went by he looked right in our window and really stared at the abacus on [redacted] windowsill.'

(U) Well, [redacted] desk is in a prime location, right near where the entry passageway narrows and the RP (royal party) would have to go single file. That's where I stationed myself for when they emerged 20 minutes later. I was well rewarded because they did indeed go single file, the Q went zooming past straight out to the Rolls, but the P stopped AGAIN and REALLY STARED at this little doodad on the sill, then looked up AT ME and pointed at the thing and gave me a quizzical look. Well, all I could muster in that instant was one of those "I Love Lucy" type shrugs. Afterwards I said 'oh how rude and we really should write to the poor man and explain what it was.' So I wrote and told him it was a child's wooden abacus and that we DO usually use more sophisticated equipment. (b)(3)-P.L. 86-36

(U) The Prince's staff person (Brigadier Miles Something-Something) wrote back saying he'd shown the P my letter and P said to write and thank me. So at least my letter whizzed by royalty. If I only had the Coronation coloring book I was given in the early 50's, I could have probably sent it in and had it autographed. Lost chances. Oh well, I never finished it. I didn't know what a scepter was, let alone how to color it. So that's the real story.

(b)(3)-P.L. 86-36
(b)(6)

c. (U) PUBLISHED AUTHOR

[redacted]

[redacted] (b)(3)-P.L. 86-36

(b) (6)

[redacted] If you have always wanted to take this kind of trip or just want to read the article, a copy is available in [redacted].

7. (U) ACTION LINE

Dear Action Line:

Who is it who hands out frames for CA Professionalization certificates? In the span of a few months, one person receives his certificate in a black plastic government-issue frame, the next person receives his in an elegant wooden gold-trimmed frame, and the next person receives the certificate with no frame whatsoever!

For most people, professionalization is the only certificate that they choose to display. Are the credentials of professional cryptanalysts being exhibited equally?

Frameless in Z

(b)(3)-P.L. 86-36

ANSWER - provided by [redacted] Assistant Exec of the CA Panel

Prior to 1994, the Career Panels would supply all the frames for professionalization certificates. The Panels would frame the certificates before sending them off to the "09" organization for presentation. These frames were usually plastic, although wooden frames were used in the early '90s. Approximately one year ago, M34 informed the Panels that the funding for frames for professionalization certificates would no longer be included in their budget. The Panels were instructed to mail the unframed certificates to the "09" offices. The "09" offices have the option of supplying a frame for the certificate if they choose.

ANSWER - provided by [redacted] former CACP Exec

I would like to add to Donna's response. The length of time it takes for presentation of a professionalization certificate, once it is received in the "09" office, varies greatly, from office to office. Some recently certified people wait two, three, or more months to receive the certificate from the office chief. This delay may make the differences in the frames all the more apparent. If someone who was certified four or five months ago, and received one of the "last" wooden frames that the panel was able to obtain, is included in the same ceremony with someone under the new "frame" guidelines, there could be obvious differences in the presentation.

ANSWER - provided by [redacted]

(b)(3)-P.L. 86-36

Until recently the panels supplied frames for professionalization certificates. In [redacted] we also give out framed CMP graduation certificates. Normally, we order plastic frames in the spring for the class which graduates in August. This year we are ordering additional frames so that we can have some extras on hand for professionalization certificates. We have been able to find plastic frames for the few certificates awarded recently.

[redacted]

//

8. (~~FOUO~~) EDITORIAL CORNER

If you have a relatively short technical treatise, or anything you would like to have considered for inclusion in future issues, please submit it to any member of the editorial board or any of our office POCs.

PLEASE paragraph classify each item submitted, and USE ASCII FORMAT!

A reminder that anonymity may be requested for Action Line items - in fact, you may mail them in hardcopy form to any member of the editorial board or any of our office representatives.

We would very much like this newsletter to represent a broad cross-section of the CA community - we need some more volunteers to help us, however. Perhaps you would like to work on one of the topics in this issue, or perhaps there is another topic which you think should be included in future issues. Either way, we would like your input, and help, so give one of us a call. The more people who divide up the work, the less burden on any one person.

##
NOTE: We MUST receive any submissions for the May issue by 21 April.
##

EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum

[redacted] NCS

OFFICE Reps

(b)(3)-P.L. 86-36

[redacted]

\\\

[redacted]

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

(b)(3)-P.L. 86-36

[redacted]

(U) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:17
(U)PE EXTERNAL PAGE

[redacted] (b)(3)-P.L. 86-36

****
* TAILS OF THE KRYPT *
****
April 1995

##########
//////////

TABLE OF CONTENTS:

1. CA Perspective
2. Calendar of Events
3. Word from the CACP
4. Personnel Issues
5. Technical Health
6. Community Service
7. Puzzles and Problems
8. Literary Tidbits
9. Action Line
10. Editorial Corner

##########
//////////

[redacted] (b)(3)-P.L. 86-36

1. PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of [redacted] Z1. Although he is known as the Z Group Computer Security Manager, [redacted] primary job is Management of the Z Group Computer Budget.

CRYPTANALYSIS, COMPUTERS, and CONGRESS

Ultimately we respond to Congress in our annual activities to purchase computers for our cryptanalytic mission. Historically, this task has been a fairly straightforward process despite occasional periods of funding pressures. In recent years, however, the annual ritual of making and defending requests for supercomputer assets has become increasingly cumbersome, difficult, and stressful for those in Z Group who manage the process.

In this perspective I would like to provide you with some insights into our ability to achieve the success rate we have developed as we examine the process in a little more detail.

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted] (b)(3)-P.L. 86-36

[redacted]

It's worthwhile to look at the old procedures. We effectively produced a chart which had an exponentially increasing curve on it along with annotations stressing a documented [redacted] increase in various processing requirements. This chart was briefed at each level by a small group of technically literate cryptanalytic managers to a broad cross-section of budgetary folks who remained silent at cross-examination time for fear of exposing lapses in their knowledge bases. Furthermore, congressional oversight was minimal; our budget had few roadblocks.

And then a rather dramatic change took place in the last ten years. Publicity associated with various scandals in the Intelligence Community served to drastically increase congressional scrutiny of our budgets with the cascading result that a simple technical argument for our needs was no longer accepted at any level of the budget requirements reviews. In short, we had to quickly develop across the CA community a far-reaching strategy to create solid arguments in support of the large outlays of funds which purchase the super computers. Central to that strategy, and specifically noted by auditors, was the need to generate usage statistics for our systems.

The current solution to the statistics problem, a brilliant piece of analytic exploitation, has not yet received the recognition it deserves. Its vision is on a global scale. Its creation and successful implementation is an example of cross-disciplinary talent working together to reach a common goal. Simply put, a small CA team formulated and executed a multi-pronged coordinated effort to generate solid computer usage statistics and educate the appropriate players in the game. And with CA resources, it was able to perform this task with minimal bureaucracy and interference.

First a large program was written to perform target forecasting based on vary sparse statistics. Fortunately only one Cray was dedicated to this task. Second, a covert team approached a friendly target head-of-state to employ increasingly difficult enciphered communications in their systems whose exploitation data could feed this program. A second Cray was dedicated to collect and process the resulting high data rate signal (we were assured that one channel would always contain CNN video news data). Thirdly, a political action team was dispatched to make sure this target country continually appeared on the White House most critical requirements list. There was no need for a third Cray here, merely the unwitting cooperation of two other government agencies. And, finally, with all parts in place, leaks were made to several sources downtown to insure congressional focus on this target. The result: continuous highest level tasking on a process which places heavy demands on our super machines, generates fundamental processing statistics, and produces unmeasurably valuable intelligence reports. (b)(3)-P.L. 86-36

All the wheels are currently turning smoothly: the analytic prediction program is generating copious charts, matrices, and figures. A brief executive summary this year condensed to an estimate of "exactly 41.769%". Truly a remarkable outcome for this well-conceived effort. A backtrack approach might be used to gain further technical insights available in a non-published treatise dealing with the LIRPA (Localized Inverse Reconstitutions in Probabilistic Applications) method as applied to Project SLOOF (Subliminal Legislative Operational Oversight Formalizations). It's a most interesting game.

//

2. CALENDAR OF EVENTS

15 April 1995	SAVVY Program Briefing, CANX Auditorium 1217 hours (see Section 3.) (b) (6)
4 July 1995	[redacted] speaks to Agency Seniors FANX IV Auditorium, 0800 - 1200 hours
31 September 1995	Retail Shops Open in OPS #1 South Corridor
1 October 1995	RIF Policy Takes Effect (see Section 4.)
FUTURE DATES	
July 1995	SAVVY Program Begins (see Section 3.)
October 1995	Ratskeller opens in OPS2B
30 February 1996	Revised CA Criteria Takes Effect

//

3. CACP NEWS

A. TECH TRACK ADDS THIRD HURDLE

Hailed as the third jewel for the triple crown of the technical world, the new SAVVY Program will complete the Agency's quest for technical leadership. Along with the Certification Program and the Tech Track, the SAVVY Program will give needed direction for those who desire to rise in a technical career.

The Certification Program determines competency; the Tech Track determines contribution to technical health; the SAVVY program will determine networking savvy. The more Agency people who know you and the higher their grades, the higher you will be rated in the SAVVY Program. There will be three Monikers in SAVVY similiar to the Titles of Tech Track: NAIVE, NOVICE, and PLAYER. The application process couldn't be easier. Just make a list of people and their respective grades whom you think know you by name and face. If you don't know to whom to give the list, you will automatically get the lowest Moniker of NAIVE. Otherwise, you may get the NOVICE Moniker (if most people know you, but they mispronounce your name) or the coveted Moniker of PLAYER.

Note that, in keeping with the spirit of the times, you need not actually be productive to attain even the highest rank that the Agency technical world can bestow: Certified Master Player.

B. CRYPTANALYST CONSIDERS CALLING IT QUITS AFTER CONFIRM CONFRONTATION

The CA Panel's newest intern, Ms. Pauline Pitt, has reported that she may offer her resignation after being on the job for only two days. On her first day at NSA, Ms. Pitt confidently approached the CONFIRM post with her new badge. The reader accepted her badge, which was worn around her neck, and she punched in her secret PIN number, but the reader would not release the badge. Ms. Pitt, wanting to obey the reader's order to PROCEED, ducked her head, slipped the

(b) (3)-P.L. 86-36

[redacted]

chain over her head, stepped off the mat, and was immediately arrested by the attending FPS officer for not wearing her badge. She explained what had happened, but examination of the reader showed no sign of badge or chain. The officer suggested she call her office for identification. However, Ms. Pitt was unknown there to anyone save her supervisor, who arrived for work at a later time. She was taken to FPS Headquarters, where she was held and questioned for several hours until her supervisor arrived to vouch for her. The badge was eventually discovered in the bowels of the reader. It is now known that the secret number, inadvertently assigned, was one of those keyed to apprehend individuals wanted for various infractions of Agency rules.

//

4. PERSONNEL ISSUES

A. CRYPTANALYSTS AND THE RIF

The task force which formulates and implements the Agency's RIF policy, should it ever be needed, has submitted its decisions for presentation to the NSA work force. The group first considered that a Lottery system would be the fairest way to determine who would be riffed. However, it was thought that the Agency's needs would be better suited if each career field had its own RIF Program and Criteria. The following are the new guidelines for the Cryptanalysis career field.

Any Cryptanalyst shall immediately be eligible for RIF processing who:

1. Cannot correctly spell CRYPTANALISIS on the first try.

2. Cannot solve the Sunday BALTIMORE SUN Jumble puzzle in one (1) day.

3. Is unable to walk from TFCU at OPS #1 to TFCU at VCC without going outdoors.

4. Does not demonstrate dedication to the field by maintaining a FULL set of SHARPENED colored pencils. (It is realized that this requirement may be a little out of date. It will be updated as soon as all SUNs have the PAINTBRUSH Accessory installed.)

5. Has not shown his/her well-roundedness by becoming certified in at least five other fields, including Programming, System Administration, Data Flow, Computer Operator, and Destruction Officer. (Persons weighing more than 200 pounds will be considered to have automatically fulfilled the well-rounded requirement.)

B. QUICKIE PERSUM TIPS ON HOW TO GET PROMOTED:

* Reading Achievements -- This is the most overlooked and the least well done part of most Persums. But very often, the content of this item makes the critical difference in a promotion decision. List "TQM JOURNAL", "DRESSING FOR SUCCESS", and "DAYTIME SOAPS", as your regular reading, and wait for the whispers to start around the office coffee mess.

(b)(3)-P.L. 86-36

9/23/2010

* Summary of Previous Experience -- Most people don't fully appreciate the fact that Persums are signed by supervisors who are only attesting to the truth of the Current Assignment. So, to get that all important leg up in the promotion process, consider attribution-free embellishment on the Summary of Previous experience section. You'll be pleasantly surprised at the spectacular results!

//

5. TECHNICAL HEALTH

A. ZENTOOLS - YOUR ANSWER IS HERE!

(U) Stress is a major topic of concern not only in our Agency but in private corporations. Take a moment to reflect on the number of items on your daily agenda. Personally, my schedule of events for one week would take the breath away from a "busy" person of one hundred years ago. I am "happy" to report to you that it seems that Mahayana Software, Inc. of Calm Springs, Florida, may have hit on the perfect product...ZENTOOLS.

(U) After spending some time with this product, not only did I find it extrememly effective, I must commend the developers for their insight, creativity, and genuine sensitivity for the sanctity and importance of individual beliefs. What surprises me is that a relatively small corporation would risk developing a product so potentially controversial. A bold move, indeed, but one which not only individuals, but employers are raving about. Listen to these testimonies:

"I was so stressed at work and home that it seemed I had lost control. I tried the spas, hobbies, church, but nothing seemed to work. Then I was in the computer store one day and purchased this package, ZENTOOLS. It changed my life!"
- Bob: Computer Programmer, Boston, Massachusetts

"Before ZENTOOLS, our office was a den of backbiting, coffee swilling, doughnut munching yuppies. I can't believe the change! There is no noise any longer, productivity is up 35% and climbing, our customers aren't sure they still deal with the same people. Everyone is friendly, healthy, heck...nine people have even quit smoking! It is the single best investment our company has ever made!"
- Stephanie: V.P., Eastern Marketing/Sales Conglomerate, New York.

(U) Briefly, ZENTOOLS is designed to teach the user how to develop and maintain periods of productive meditation while at work, home, or traveling (but not driving). There are seemingly innumerable options which you can set. You can even set it to come up randomly during your day, but at least a minimum number of times, which you select! Sessions may vary widely but in general consist of a reflective period, a teaching period where lessons of self discipline and control are conveyed to the user, an agenda period on prioritizing your projects which you will do immediately after your session and, finally, the self induced trance. (Note to Employers/Managers: It is highly recommended that you establish some trance position guidelines such as whether it is acceptable for employees to lie down, sit on floors, etc... . The documentation accompanying the software is very helpful in this regard.)

(b)(3)-P.L. 86-36

Doc ID: 6823790

(U) Supervisors have been made aware of this product and can arrange demonstrations through NCS. Your feedback could be a key in making this product available to all Agency employees. Remember the name, ZENTOOLS, and have a peaceful day!

B. LEONARDO WHO?

Certain famous first names are almost universally recognized and, to a lesser degree, associated with not-so-famous last names. Take Galileo. Most people associate Galileo with the gastronomical telescope and some even know that his last name was Galilei. It has been rumored that as he became a more seasoned astronomer, he changed his last name to Galilee. How about Marco? In his time, he was a big shot who, when properly oriented, landed on inventing the Poloroid camera. Michaelangelo Buonparroti painted flora and fauna on the ceiling of a once pristine chapel. And then there's Leonardo Pisano. Leonardo Who? PISANO! You might guess that he was a vintner and early forbear of the widely known Carlo Rossi, but what he's actually noted for was observing that the birth rate of rabbits follows a particular pattern. He subsequentially became famous, and was later known as FIBONACCI.

//

6. COMMUNITY SERVICE

A. RATSKELLER TO OPEN IN OPS2B

Have you noticed how creative sparks fly when you are out with friends drinking your favorite brew? Up to now, there was no place where cryptanalytic subjects could be freely discussed while enjoying the golden beverage with good company. Imagine how much cryptanalysis could benefit by having such a place in a secure environment where classified discussions were encouraged!

Well, your wait is over. The BOD, ever committed to the precepts of TQM, have heard your cries! Part of the basement of OPS2B will become the world's first classified Ratskeller. Current plans are to decorate to the theme of CASABLANCA. Agency seniors will take turns as waitpersons, donning costumes of the WWII era and using nicknames such as "Fast Freddie" and "Ace Perkins". Hours of operation are expected to be 0500-1330 Mon & Thurs (to accommodate early people), 1030-1800 Tues & Fri (for late people), 0000-0430 Wed (the red-eye special for Mids). You can expect to start sipping the suds sometime in late October of this year.

B. NEW SHOPS AVAILABLE TO WORK FORCE

With the reductions in the Agency work force, unused office spaces have appeared in OPS #1 South corridor. CWF announced at its Saint Patrick's Day luncheon that new shops will soon be available to the Fort Meade Campus work force. Plans for a discount liquor store (similar to Class 6 stores), ABC Pawn Shop, and Betty's Briefing Clothing Store, are being finalized. Although not yet on a par with the shops at Pentagon City, CWF feels that these retail outlets will improve the quality of life at NSA. Free samples, complimentary hot dogs and lemonade, and balloon rides from outside Gatehouse #4, will mark the grand openings on 31 September 1995.

//

(b)(3)-P.L. 86-36

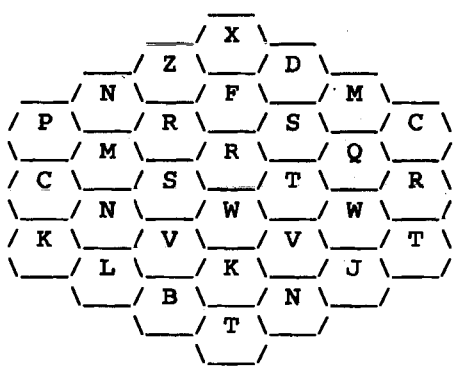
9/23/2010

7. PUZZLE AND PROBLEMS

A. PUZZLE (Send your solution to our Puzzle Editor, [redacted] and we will publish the names of all those who solved this one.)

(b)(3)-P.L. 86-36

As a challenge, form as many common English words as you can of 5 or more letters from the diagram below. Please start at any letter, but move only to adjacent letters. Repeating a letter by staying on it is not permitted. If you wish, however, you may return to a letter after moving off of it. Lastly, the following are not allowed: foreign words; obscure words; out-of-date words; less commonly used words; slang.



B. PROBLEMS

Q: How many Windows programmers does it take to change a light bulb?

A: Four Hundred and seventy-two. One to write WinGetLightBulbHandle, One to write WinQueryStatusLightBulb, one to write WinGetLightSwitchHandle...

Q: How many WordPerfect support technicians does it take to change a light bulb?

A: We have an exact copy of the light bulb here, and it seems to be working fine. Can you tell me what kind of system you have? OK. Now, exactly how dark is it? OK, there could be four or five things wrong...Have you tried the light switch?

Q: How many managers does it take to change a light bulb?

A: We've formed a task force to study the problem of why light bulbs burn out, and to figure out what, exactly, we as supervisors can do to make the bulbs work smarter, not harder.

Q: How many testers does it take to change a light bulb?

A: We just noticed the room was dark; we don't actually fix the problem.

Q: How many Microsoft technicians does it take to change a light bulb?

A: Three. Two holding the ladder, and one to screw the bulb into the faucet.

Q: How many MIS (Management Information Systems) guys does it take to change a light bulb?

(b)(3)-P.L. 86-36

[redacted]

A: MIS has received your request concerning your hardware problem and has assigned your request service number 39,712. Please use this number for any future references to this light-bulb issue.

Q: How many C++ programmers does it take to change a light bulb?

A: You're still thinking procedurally. A properly designed light-bulb object would inherit a change method from a generic light-bulb class, so all you'd have to do is send a light-bulb-change message.

Q: How many developers does it take to change a light bulb?

A: The light bulb works fine on the system in my office...

Q: How many shipping department personnel does it take to change a light bulb?

A: We can change the light bulb in seven to ten working days, but if you call here before 2 P.M., and pay an extra $15, we can get the bulb changed overnight.

Q: How many Microsoft Engineers does it take to change a light bulb?

A: None. [redacted] will just redefine Darkness(tm) as the new industry standard.

(b) (6)

Q: How long does it take a DEC repairman to change a light bulb?

A: It depends on how many burnt-out bulbs he brought with him.

Q: How many Newton* users does it take to change a light bulb?

A: Foux! there to eat lemons, axe gravy soup.
*Newton is an Apple hand-held Personal Digital Assistant (PAD) computer that recognizes handwriting and speech.

Q: How many Microsoft vice presidents does it take to change a light bulb?

A: Eight. One to work the light bulb, and seven to make sure Microsoft gets US$2 for every light bulb ever changed anywhere in the world.

Taken from the "Illuminating Geek Jokes" section of WIRED magazine (Dec '94):

//

8. TIDBITS

A. THE WAIL OF A CRYPTANALYST
by W.M.V. Hoffman

There are moments when the world looks bright and rosy,
When the messages are tailing as they should,
When each fancy little letter
Makes the columns come out better,
And the rows could act no better if they would.

Then the heart of the cryptanalyst is merry,
And he chortles as he sets the traffic down;
And he thinks the enemy chaps
Are such simple-minded saps,

(b) (3)-P.L. 86-36

[redacted]

And the man who makes their ciphers is a clown.

But, alas! there comes a day of horrid failure;
Our cryptanalyst is miserable and blue;
  And the nasty little letters
  Thumb their noses at their betters
And make gibberish no matter what you do.

You can stand them on their heads and read them backwards,
You can shift them left to right and to and fro,
  You can calculate and mutter
  Till your brain becomes like butter,
But no matter what you try it doesn't go.

Then you curse the day when ciphers were invented,
And you kick yourself around for being dumb;
  And the guy who once invented
  Such a code is a demented
Low-down, slinky, lousy, dirty, rotten bum!

(From the Feb 1982 issue of Cryptolog)

B. MEMORABLE QUOTATIONS

Jim Koch, Founder of The Boston Brewery and maker of the Samuel Adams line of beers was overheard to have said recently:
"There is food in beer, but there is no beer in food. Beer is like liquid bread - it provides the same necessary nutrients. I say, just lay off the food."

"Smoking kills. If you're killed, you've lost a very important part of your life."
- Brooke Shields, said to demonstrate why she should become spokesperson for a federal anti-smoking campaign

"I've never had major knee surgery on any other part of my body."
Winston Bennett, University of Kentucky basketball forward

"I support efforts to limit the terms of members of Congress, especially members of the House and members of the Senate."
- Vice-President Dan Quayle (surprise, surprise)

"Outside of the killings, Washington has one of the lowest crime rates in the country."
- Mayor Marion Barry, Washington, D.C.

On Pesticides:
"Sure, it's going to kill a lot of people, but they may be dying of something else anyway."
- Othal Brand, member of a Texas pesticide review board, on chlordane

"The exports include thumbscrews and cattle prods, just routine items for the police."
- Commerce Department spokesman on a regulation allowing the export of various products abroad

"Are you any relation to your brother Marv?"
- Leon Wood, New Jersey Nets guard, to Steve Albert, Nets TV commentator

(b)(3)-P.L. 86-36

9/23/2010

"If you can't make the putts and can't get the man in from second on the bottom of the ninth, you're not going to win enough football games in this league, and that's the problem we had today."
- Sam Rutigliano, Cleveland Browns coach, on why his team lost

On Government Ability to Communicate After Death:
"Beginning in February 1976 your assistance benefits will be discontinued...Reason: it has been reported to our office that you expired on January 1, 1976."
- Illinois Department of Public Aid

On Criticism:
"That lowdown scoundrel deserves to be kicked to death by a jackass--and I'm just the one to do it."
- a congressional candidate in Texas

"It takes a virile man to make a chicken pregnant."
- Perdue chicken ad, as mistranslated abroad

MEMBERS AND NON-MEMBERS ONLY
- sign outside Mexico City's Mandinga Disco in the Hotel Emporio

Wish---To end all the killing in the world
Hobbies---Hunting and fishing
- from personal statistics of California Angel Bryan Harvey, flashed on the scoreboard at Anaheim Stadium

"He's trying to take the decision out of the hands of twelve honest men and give it to 435 Congressmen!"
- Representative Charles Vanik of Ohio, when he heard that the indicted Spiro Agnew was asking to have his corruption case tried by the House instead of in a regular court

"The Holocaust was an obscene period in our nation's history...this century's history.... We all lived in this century. I didn't live in this century."
- Dan Quayle, then Indiana senator and Republican vice-presidential candidate during a news conference in which he was asked his opinion about the Holocaust

"In the early sixties, we were strong, we were virulent..."
John Connally, Secretary of Treasury under Richard Nixon, in an early seventies speech, as reported in a contemporary "American Scholar"

"At the Lincoln Park traps on Sunday...over 80 shooters took part in the program. Rotarians, be patriotic! Learn to shoot yourself."
- from Chicago Rotary Club journal, "Gyrator"

"The streets are safe in Philadelphia, it's only the people who make them unsafe."
- Frank Rizzo, ex-police chief and mayor of Philadelphia

"I've always thought that underpopulated countries in Africa are vastly underpolluted."
- Lawrence Summers, chief economist of the World Bank, explaining why we should export toxic wastes to Third World countries

On the Little-known Importance of Poultry Inspectors:

(b)(3)-P.L. 86-36

"The crime bill passed by the Senate would reinstate the Federal death penalty for certain violent crimes: assassinating the President; hijacking an airliner; and murdering a government poultry inspector."
- Knight Ridder News Service dispatch

"After finding no qualified candidates for the position of principal, the school department is extremely pleased to announce the appointment of David Steele to the post."
- Philip Streifer, superintendent of schools, Barrington, Rhode Island

"The doctors X-rayed my head and found nothing."
- baseball great Dizzy Dean explaining how he felt after being hit on the head by a ball in the 1934 World Series

C. LIMERICKS

A manual cryppie did so laugh
And smile as he worked on his digraph.
He thought ZQ meant `beating',
But it really was `meeting';
So the message read `beating his staff'!

A psychic cryptanalyst poses
To solve systems by crypto-osmosis.
He could dream in the night,
Which solutions were right,
Then leave early to tend to his roses!

The gymnast cryptanalyst Fred,
Decrypts while he stands on his head.
But the problem, you see,
Was with TOPIs, 'cause he
Made plain text that upside-down read!

//

9. ACTION LINE

A. QUESTION #1

Dear Action Line,
"Tales of the Krypt" recently reported that the CA Professional Qualifications Examination (CAPQE) will no longer be required for certification as a professional Cryptanalyst at NSA. Are any other changes being planned to the certification requirements? If so, what are they?

CA (Curious Analyst)

Dear CA,
The elimination of the CAPQE is just one of the changes being planned for the CA certification process. The Panel - in conjunction with M3, the General Counsel, and a special DDO Legal Affairs Committee - has been busy reviewing all professionalization criteria, looking for weak spots. Doing away with the CAPQE is only the first to be put into effect. Some other changes to be implemented:

1. A number of additional NCS courses will be required. The growth in the types and sophistication of communications in recent years has meant that new courses were going to be developed anyway, and the Panel was quick to recognize these courses as a

(b)(3)-P.L. 86-36

9/23/2010

way to fill the gap left by the CAPQE. It is expected that 20-25 required courses would be added to the current number of 14. As a bonus, many of the new courses are expected to have applications to actual operational cryptanalytic problems.

2. Revival of the "points" system, where specific accomplishments are awarded some number of points, and professionalization is achieved when a set threshold is reached. This program will differ from similar versions in the past, however, in that the number of points needed for certification - and the number of points awarded for specific accomplishments - will be tailored to each aspirant, as determined by a series of interviews with Panel members. In this way, we hope to address the all-too-common situations where some people appeared to attain professionalization more rapidly than others. [This approach is very familiar to the sporting world, especially in golf, bowling and horse racing.] This is designed to "level the field", giving some aspirants a better shot at gaining certification.

3. The writing of a technical paper will still be required, but the review process will be eliminated. Aspirants will no longer be required to give an oral presentation of their paper (this was found to be too stressful for the reviewers), but will instead be asked to sign an affidavit that the paper being submitted deals with a valid cryptanalytic topic, is of a minimum length (to be determined later), and took a minimum amount of time to write (also to be determined later). This affidavit will become part of the aspirant's permanent record with the Panel, and if at some time in the future the paper is actually read and found not to be in compliance, the Panel will have the power to strip the analyst of their certification.

4. In recognition of the crucial role that computers have come to play in cyptanalysis, the requirement of a computer program will also be modified. The primary aspects of the new criteria are: a) three programs will be required (vs. the current requirement of one); b) to promote standardization, all programs must be written in either Ada, C++, FORTRAN77 or QBASIC; c) again to promote standardization, all source code must be created using the emacs text editor; and d) programs must compile and run on a minimum of three different platforms (e.g. IBM PC, SUN and CRAY). Programs must be completely orignal and will be subjected to a rigorous review by a panel of computer experts. Any program found to contain routines written by others (to include most standard library subroutines) will be rejected.

That just about covers it. There are a few other changes being planned, but you don't need to be concerned over them. As you can see, the Panel is vitally concerned about the continued technical health of the field of Cryptanalysis, and it is hoped that the new criteria will not damage our posture to any great extent. As always, if you have any questions about the new process, you may bring them to the Panel, and they will give them the attention they merit. Thanks for the question.

[redacted] CACP

B. QUESTION #2 (b)(3)-P.L. 86-36

Dear Action Line:
Maybe I'm dumb, but I don't have a clue as to why the Agency cares

[redacted]

about VISION STATEMENTs all of a sudden. It seems to me to be such a waste of time and effort.

Non-visionary

Dear Non-visionary:

You couldn't be more wrong! Vision statements are the driving forces of change in an organization. They give full purpose and direction to the mission of any group. They set the tone for the hoi polloi.

To give you an example, suppose we talk about a company which makes widgets. This company came up with the vision statement: TO MAKE THE BEST POSSIBLE WIDGETS. You probably think that such a profound statement took years to evolve. Actually, it took only two dozen top corporate executives two weeks to develop it during an off-site team-build in Hawaii. That single vision statement spurred the Advertising Department to come up with: TO CONVINCE PEOPLE TO BUY MORE WIDGETS THAN THEY NEED. You can see the trickle-down effect now. Even the Research Department threw its hat in the fray with: TO DESIGN TOMORROW'S WIDGETS (that's just like researchers to come up with something that allows them to procrastinate for another day). The workers decided on their own version: TO MAKE THE LARGEST SALARY POSSIBLE WHILE MAKING THE FEWEST POSSIBLE WIDGETS. As you can plainly see, the proper framing of a vision statement keeps the intricate parts of any organization working at cross vision statements instead of at cross purposes.

C. QUESTION #3

Dear Action Line:

I have noticed that, for the past 20 years, the quality of dress at the Agency has declined dramatically. The way people dress today disgusts me so much that I sometimes feel physically ill. Don't these people know that to be true professionals, they must dress appropriately? Is there anything that can be done -- perhaps the institution of a dress code?

Sore Eyes

Dear Sore Eyes:

We brought your letter to the attention of Mr. Otto Nobetter, chief of protocol. He discussed your concerns with several other senior Agency officials who jointly responded as follows:

"Complainers like you have nothing better to do than whine about silly, irrelevant things. If you worried half as much about your own productivity, it would never occur to you to be so droll. You should be more concerned about national issues, such as television prime time network ratings, the rising cost of cable television subscriptions, and famous trials from the west coast. So, dress down and take your work more seriously. GET A LIFE, Sore Eyes!"

//

10. EDITORIAL CORNER

We hope you have enjoyed reading the first April Fool's issue. It was meant to bring enjoyment and a little smile into your very technical world.

##
NOTE: We MUST receive any submissions for the May issue by 21 April.
##

CONTRIBUTORS:

[redacted] (b)(3)-P.L. 86-36

OFFICE Distribution Representatives [redacted] (b)(3)-P.L. 86-36

\\\

TOP SECRET//COMINT

~~(C)~~ *POC:* [redacted] *info*
(U) *Last Modified: 10/30/2002 11:42:18*
(U)PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
MAY 1995

##########
//////////

~~(FOUO)~~ TABLE OF CONTENTS:

1. CA Perspective from [redacted] Chief, R51
2. Calendar of Events
3. Word from the CACP
   a. New CACP Member
   b. Announcement of Positions in CA Development Programs
   c. CA Cross-Training Program
4. Technical Article on Mini-Scamp '95
5. Community Service
   a. Z FWP Monthly Video Presentations
   b. NSA Science & Engineering Presentation
   c. First Offering of Cryptologic History Course
   d. [redacted] Telecommunications Technology Forum
   e. Tech Trend Notes
   f. MEPP
   g. WiMS Activities
6. Action Line - Limiting Terms of KRYPTOS Officers
7. ANNIVERSARY CONTEST

(b)(3)-P.L. 86-36

##########
//////////

1. ~~(FOUO)~~ PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of [redacted] Chief, R51.

(b)(3)-P.L. 86-36

~~(FOUO)~~ R51 is the Mathematics Research Division of R5. There's a lot going on in R51 besides our basic research work but I'm not sure that very many people really understand the diversity of activities here. Since the whole idea of all these projects is to support the cryptomath community at NSA, I thought it would make sense to tell you about the whole range of projects going on in R51 and also try to convince you that R51 is a great place for a cryptanalyst to take a diversity tour. Let's start with the latter topic.

~~(TSC)~~ MATHEMATICS RESEARCH: This is our core mission: to carry out research on math problems relevant to any aspect of the Agency's SIGINT or

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

INFOSEC missions. Most of our work is related to cryptologic mathematics and supports Z Group cryptanalysis efforts, but we are also trying to have an impact on problems involving collection, processing, [redacted] but this is an area where we need to increase our contribution.

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

Whether you have a PhD in math or a BA in English you are welcomed and encouraged to stop in any time and talk about a diversity tour in R51. The role of mathematics in cryptanalysis is well known, and a tour in R51 gives you a chance to extend your math expertise into some exciting new areas. Recently we have had a large research effort [redacted] jump off onto another aspect of R51. But, before I go on, please consider coming to R51 for a diversity tour - there is a great group of people here to work with and we are equally happy to learn from you as well as teach!

(S) R51 MANAGEMENT: I want to give you an overview of some of the other activities going on in R51 but first, I'll mention that the management structure of R51 is much simpler than in most organizations. At the moment, other than the chief, we have only two people in management roles. [redacted] is the Technical Director of R51 and has the job of bringing new projects into the office and making valuable technical contributions to all of the projects. He organizes the R51 work force into effective teams and acts as our main interface to the folks we are trying to support. [redacted] is our External Research Director, and takes care of coordinating all of the R51 activities that support the mathematics infrastructure of the U.S. as well as the projects that involve support to the NSA cryptomath community by folks from the academic and industrial world. He makes sure that a complicated set of

(b) (3)-P.L. 86-36

[redacted]

actions move forward in a timely manner throughout the year, plans out the R51 budget (which supports the whole cryptomath community in many different ways), and formulates research projects for external work. Other than myself, [redacted] there are no other managers of any sort at the moment, just 40 or so mathematicians (including visitors) who are left free to do math. We usually have a customer deputy visiting from Z and most recently this was. [redacted] has moved on to take over as the acting Chief of R53.

(C) THE DIRECTOR'S SUMMER PROGRAM: We bring 25 of the very best undergraduate math majors in the country to NSA each summer through this highly competitive program. Usually 10 are returning DSPers from previous summers and they are assigned to offices throughout the cryptomath community, and 15 are first time DSPers who work down in the DSP room under the mentorship of top Agency cryptomathematicians. The goal here is to establish a long-term relationship with the mathematicians who will be the leaders of the U.S. math community for the next generation. (We will hire some former DSP students here (and have hired some at IDA) but that is not the primary goal.) The program manager for the DSP is [redacted] and she handles every aspect of the complicated process of advertising the DSP, organizing the selection meetings, and tracking a large pool of students through the clearance process. She has the whole process running very smoothly and we are very excited about this year's group. It is extremely important to have a strong presence by Z in the DSP room and this year we are very happy to have [redacted] as the DSP Technical Directors.

(FOUO) THE MATHEMATICAL SCIENCES PROGRAM: This is a program through which NSA funds undirected mathematics research in the U.S. academic community. [redacted] is the MSP director and [redacted] the program administrator. The MSP, which also funds conferencess and workshops, has had a major impact on the U.S. math community and has played a large role in promoting a positive image for the Agency. A committee of the AMS oversees which grants are funded and the program has enabled many younger mathematicians to get funding. A current action item here is to get more of the mathematicians receiving grants to visit NSA and lecture on their work.

(FOUO) THE SABBATICAL PROGRAM: In addition to the MSP, [redacted] and [redacted] also manage the Sabbatical Program which brings academic mathematicians into NSA for a year or two. This program has a been a great success. At the moment [redacted] is visiting on the sabbatical program and working in R21. This summer three people who originally visited through the sabbatical program will return for the summer: [redacted] In June [redacted] will start a sabbatical tour and in the fall [redacted] will arrive for a year. This program has been extremely valuable for two reasons. First, we get some first-class help on our most difficult problems. Second, we build some strong ties to the academic world. For example, [redacted] is helping us establish a Center for Computational Mathematics at Rice University which will play a large role in our outreach efforts to the Hispanic mathematics community.

(FOUO) JSAG: THE JOINT STATISTICAL ADVISORY GROUP: This program, which has been in existence for 20 years, brings unclassified statistics problems of operational interest to three leading centers of statistics research: Stanford University, U.C. Berkeley, and the University of Washington. Work carried out on these problems appears in a series of reports that are available through R51. The JSAG problems have been the

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

topic of many PhD dissertations at the three institutions listed above. A related activity is the sponsoring of applied mathematics workshops and a recent example is the conference on applied change point theory organized by [redacted]. Conference proceedings are now available. If you can formulate a statistics research problem in an unclassified setting and would like some help, call [redacted] or [redacted]

(FOUO) MATHEMATICS CONSULTANTS: Leading academic mathematicians regularly visit the Agency through R51 and work here and in operational areas. Among our regular consultants are [redacted] from Clemson, [redacted] from NC State, and [redacted] from UMBC. [redacted] who visited through the sabbatical program, will join our list of consultants soon. We also bring [redacted] of AT&T in for consulting work.

(b)(3)-P.L. 86-36

(U) WiMS AND OTHER OUTREACH EFFORTS: R51 provides the funding and administrative support to WiMS activities (Women in Mathematics) at NSA and to a number of outreach and recruiting efforts to minority mathematicians and institutions.

(FOUO) IDA: R51 is the primary interface for the three IDA research centers that work exclusively for NSA: The Center for Communications Research at Princeton, The Center for Communications Research at La Jolla, and the Supercomputing Research Center in Bowie. The mission at SRC is moving away from an emphasis on the design of supercomputers and into the areas of advanced cryptanalytic computing and network security and exploitation. To emphasize this change the name of SRC will also change in the near future. In addition to considering diversity tours in R51 please take some time to consider a tour at any of the three IDA centers. Again, I would be glad to talk about this with anyone..

(FOUO) R51 CLASSIFIED LIBRARY: The R51 library, managed by [redacted] houses over 11,000 cryptologic mathematics papers from the past 50 years. Rachel is now responsible for the electronic distribution of IDA papers (and R51 papers soon) and is organizing a large-scale effort to put the R51 library on-line. The abstracts are already on line and you can access them by becoming a [redacted] user. Call [redacted] for details.

(FOUO) R51 SEMINAR: For many years R51 has sponsored a general seminar on current topics in cryptologic mathematics. The R51 seminar meets nearly every Thursday at 1:30 p.m. in the R51 Math Lab. Watch for the announcements. Currently [redacted] is coordinating the seminar series and he has been finding some fantastic speakers from all over the Agency.

(U) OK - I have run out of steam for now, but if you got this far thanks for taking the time to read about R51. We are here to serve the whole cryptomath community so come over and get involved with some of our activities.

(b)(3)-P.L. 86-36

****

//

2. (FOUO) CALENDAR OF EVENTS

May 1-5 ACE (CCR Princeton)

[redacted]

May 3	CLA Speaker "Language Policies in the United States" (OPS2B 4118, #6, 1300)
May 8	Z Technology Forum; "An Inside Look at the [redacted] (FOUO)"; by [redacted] (1300-1400, OPS2B 4118 Rm.6)
May 9	NSA Science & Engineering Society Talk, "Stopping Terrorists in MidAir with Aviation Security Technology", (R&E Symposium Center, 1000) (b)(3)-P.L. 86-36
May 10	[redacted] Telecommunications Technology Forum, (Friedman, 1000 - 1600) (See Community Service for details)
May 11	Brown-bag Lunch Video, sponsored by Z FWP, "Taking Care of Ourselves and Our Parents", (2C086, 1100)
May 15	Seminar on "Bent and Other Highly Non-Linear Boolean Functions" (see 4a)
May 23	Crypto-Linguistic Association Banquet (Ft. Meade Officers' Club, 1130-1330)
May 23-25	CA PQE

PLAN AHEAD

June 1	CMI Banquet (BBC, 1830-2300)
June 1	MATHFEST 95
June 5-9	CA-305
June 20	KRYPTOS Talk (Speaker To Be Announced)

3. WORD FROM THE CACP

a. (U) The Cryptanalysis Career Panel welcomes its newest member, [redacted] to the Panel.

b. (U) The CA Career Panel will be advertizing several positions for its development programs. Five CA Intern positions and five Cross-Training positions will be advertized in the 15 May edition of the Headquarters Vacancy Announcement booklet.

c. ~~(FOUO)~~ CRYPTANALYSIS CROSS-TRAINING PROGRAM (CACTP) BEGINS (b)(3)-P.L. 86-36

The Agency cross-training program began in March, with Cryptanalysis participating as an "emerging" career field. This involves a competitive selection process whereby people who are in "diminishing" fields can apply for cross-training in an "emerging field." Once selected, the participants will have an indiyidualized

[redacted]

plan developed for them based on their backgrounds, past Agency experience, and other considerations. This plan will include coursework and diversity tours, and will usually last about three years.

In this first wave of applications and selections, the following three people were selected for participation in the CACTP:

[redacted] enjoys mental challenges and is looking forward to sharpening his analytical skills and using his educational background to work on cryptanalytic problems.

(b)(3)-P.L. 86-36
(b)(6)

[redacted] where she is a program analyst. Mary has been fascinated by cryptanalysis since she EOD-ed, but this is her first chance to get into the career field. She enjoys puzzles and intricate projects, and is looking forward to making a more direct contribution to the Agency's mission, after working so long in various support roles.

(b)(3)-P.L. 86-36

[redacted] with a background in mathematics and accounting. She is interested in areas where logical thinking, attention to detail, and organizational skills are required. [redacted]

Please welcome these Cross-Trainees into our career field as they tour through Z Group!

"""""""

[redacted] needs in his/her division. Each of the other participants also had valuable information to share about hardware, software, or algorithms.

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

METHODS... During the course of our work on the problems, we tested many existing programs and various computation platforms. Although we examined several ideas, the main techniques we found to

[redacted]

RECOMMENDATIONS... In answer to the $64,000 question (actually [redacted] which prompted the mini scamp, we found that although the

[redacted]

FOR FURTHER INFO... We have documented our motivations, methods, and findings in a final report which will soon be available upon request. This report contains much more detail than is appropriate for this article, yet it is quite readable, so we urge you to obtain a copy if you have any interest in depth detection. POCs are [redacted]

[redacted]

//

5. COMMUNITY SERVICE

(b)(3)-P.L. 86-36

a. (U) Z FWP Reps Presents Monthly Videos (See calendar)

On Thursday, May 11th, the Z FWP reps will be offering the second in a

[redacted]

series of Monthly Video presentations focusing on Family Issues, including Parenting, Eldercare, Childcare, and Balancing Family and Work. In this presentation, [redacted] Maryland Department of Mental Health, discusses the changing physiology and social behaviors of the aging and offers insight in dealing with the elderly.

b. (U) NSA Science & Engineering Presentation

[redacted] is the Scientific Advisor at the FAA in the area of Civil Aviation Security and is an internationally recognized expert in this field. His talk is entitled:

(b) (6)

Stopping Terrorists in MidAir
with
Aviation Security Technology

Few things are more terrifying than the thought of a commercial airliner exploding in midair.

The Federal Aviation Administration (FAA) is charged with ensuring that air travel is safe. They are responsible for identifying the terrorist threat, developing regulations, equipment, and procedures to reduce it, and conducting inspections to ensure compliance.

The FAA is now in the midst of a $35 Million research and development program to identify, develop, and exploit technologies to detect weapons and explosives, improve human performance in security, and increase aircraft survivability. Systems resulting from this research which are capable of automated explosive detection are beginning to be used internationally.

[redacted] will address these topics in his presentation. (See calendar)

c. (U) FIRST OFFERING OF CRYPTOLOGIC HISTORY COURSE

The Center for Cryptologic History (CCH) is pleased to announce that it is sponsoring IR-127, U.S. Cryptologic History, through the National Cryptologic School (NCS). The course will be held from 22 to 30 June (no class on 28 June) from 0900 to 1200 in 9A135 in the Headquarters building.

The course will examine major themes and enduring principles in the practice of signals intelligence and information systems security from the American Revolution to the present. CCH staff and guest speakers will also discuss the roles and operations of SIGINT and INFOSEC in many of the crises of the twentieth century. This is the story of how and why the U.S. SIGINT System got to be the way it is.

For information on course content, please contact the CCH at [redacted] or on e-mail at [redacted] For registration, please contact your organization's training coordinator.

d. (FOUO) [redacted] Telecommunications Technology Forum

(b) (3)-P.L. 86-36

The final presentation of the [redacted] Telecommunications Technology Forum

[redacted]

1994/95 Awareness Series is scheduled for next month. First, there will be a classified briefing in the morning, followed by an unclassified seminar in the afternoon.

BRIEFING

DATE: 10 May
TIME: 1000 - 1100
PLACE: Friedman Auditorium

[redacted]

SPEAKER: [redacted]

LUNCH: 1100 - 1200

SEMINAR

DATE: 10 May
TIME: 1200 - 1600
PLACE: Friedman Auditorium

(b)(3)-P.L. 86-36

TOPIC: "ENCRYPTION: A GLOBAL PROSPECTUS." Encryption is one of the most hotly debated topics of recent years. To what extent do governments have the right to control the privacy of telecommunications? Does the need for criminal information, obtained by intercept, weigh against the need for an expectation of privacy by world citizens. Cost, availability and readiness of equipment, worldwide, make policing and restricting commercial and private use difficult at best.

This seminar will present a review, recent trends in commercial encryption, and a prospectus of worldwide policy issues.

(b)(6)

SPEAKER: [redacted] a trial lawyer and patent attorney specializing in the law of technology and intellectual property. He represents domestic and foreign clients throughout the U.S. and abroad in complex technology-related cases. Formerly an Associate Professor of Electrical Engineering and Computer Science at GWU, he developed an engineering course entitled "Telecommunications Security," and a graduate law course entitled "Electronics and Computers: Patent Law Practice." [redacted] also has advised on and analyzed high-technology electronics for CIA.

OPEN SEATING, MUST BE CLEARED TS/SI-TK FOR MORNING BRIEFING

(b)(3)-P.L. 86-36

[redacted]

[redacted]

[redacted]

Calendar of Events

The following conferences and exhibitions are sponsored by NSA, academia, and professional associations. These conferences and exhibitions provide the participants with technical information and exchanges on current plans, programs and developments. Call the number listed for further information about the conference or contact [redacted] with suggestions, updates, and/or additions to Calendar of Events.

(b)(3)-P.L. 86-36

May 95

6-11 May; Digital Equipment Computer Users; Washington, DC; (800) 332-8755

8-9 May; Technology Convergence 95, Capturing Competitive Advantages Through Integrated Telecommunications Solutions; Philadelphia, PA; (800) 626-1796

8-10 May; IEEE Symposium on Security and Privacy; Oakland CA; Email: sp@itd.nrl.navy

8-11 May; ECF95, Eastern Communications Forum; Washington, DC; (312) 938-3500

9 May; 1995 Vital Issues Symposium, Geo-Political Impacts of C4I in the 21st Century; Washington, DC; (703) 757-1466

9-11 May; IN `95, 1995 IEEE Intelligent Network Workshop; Ottawa, Canada; (905) 615-6486

9-12 May; ICASSP `95; Detroit, MI; (517) 663-7114

9-13 May; 7th International Conference on Indium Phosphide and Related Materials; Hakkaido, Japan; (908) 562-3893

14-17 May; 1995 IEEE/LEOS Workshop on Interconnections Within High Speed Digital Systems; Santa Fe, NM; (908) 562-3894

15-16 May; C4I Networking Solutions -- Today and Tomorrow; Tidewater Chapter, Hampton, VA; (804) 764-7065

15-17 May; Test & Evaluation Under the New Acquisition Reform Initiatives; Washington, DC; (310) 534-3922

15-18 May; 6th Joint European Networking Conference: Bringing the World to Desktop; Tel Aviv, Israel; Tel: 31-20-639-1131

15-20 May; SVIAZ `95, 7th Biannual Communications Systems and Facilities; Moscow, Russia; (800) 868-9761

16-18 May; 7th Wireless Data Communications conference; (203) 847-5131

16-19 May; 7th Annual Canadian Computer Security Symposium; Ottawa,

(b)(3)-P.L. 86-36

[redacted]

Canada; (613) 991-7656

21-26 May; CLEO/QEL - Conference on Lasers and Electro-Optics and Quantum Electronics and Laser Science; Baltimore, MD; (908) 562- 3893

22-24 May; Information Security Conference: Securing the Extended Enterprise; Rosemont, IL; (800) 808-EXPO

22-24 May; IWANNT `95 - International Workshop on Applications of Neural Networks to Telecommunications (IWANNT `95); Stockholm, Sweden; (201) 829-4929

27-29 May; IEEE International Symposium on Requirements Engineering; Heslington, York, United Kingdom; Email: mdh@minster.york.ac.uk

****

f. ~~(FOUO)~~ MEPP HONORED

The Math Education Partnership Program has been selected to receive Special Recognition in the nationwide 1995 Public Service Excellence Award Program. All MEPP volunteers are cordially invited to attend an award presentation and social on Tuesday, 2 May from 1300-1400 in the Canine suite. Please come and share in the excitement! POC is [redacted]

****

g. ~~(FOUO)~~ WiMS Activities

At the last WiMS meeting on 20 April 1995, [redacted] (Ch, R51) provided a report on the funding support provided by R51 to external WiMS type activities. Last summer, R51/WiMS provided support to the now well known and publicized Research Experience for Undergraduates (REUs) at the Mills Summer Math Institute. This provides research opportunities for undergraduate women in mathematics. The Mills program is being funded by NSF this year. This summer, we are providing significant support for a similar program to be started up at George Washington University. Our own [redacted] will be teaching a 3 week combinatorics course there as well. In addition, R51/WiMS is providing some support to a similar REU being started this year at St. Olaf/Carleton College.

(b)(3)-P.L. 86-36

Last year [redacted] traveled out to Mills to see what this REU was all about. That was very fortunate for us since she made contact there with [redacted], a spectacular mathematician who will be EODing to NSA shortly. We hope to again send Agency representatives to Mills this year, and to St. Olaf/Carleton as well.

****

//

6. ACTION LINE

QUESTION: Has any consideration been given to limiting the terms in office of KRYPTOS officers? This would include the term in a particular office and consecutive terms of service in any office.
Signed, Anonymous

~~~~~~

ANSWER: Coincidentally, the KRYPTOS Council is in the process of considering shortening the terms of its officers. We were prompted by

(b)(3)-P.L. 86-36

[redacted]
~~~~~~

two considerations:

a) several officers serve four years and that gets to be somewhat long; and

b) we desire to get more people active in KRYPTOS affairs; increasing the turnover rate of our officers will accomplish this.

The terms of offices are defined in the bylaws and so these would have to be changed by vote of the membership. The Council plans to finalize the proposed changes at our April meeting and have the membership vote on them at the June KRYPTOS talk. To this point we had not considered prohibiting back-to-back terms of office but I will now have the Council consider this possibility. Thanks for your suggestion.

[redacted] (b)(3)-P.L. 86-36
KRYPTOS President

//

7. (TOUO) NEWSLETTER ANNIVERSARY CONTEST

It is hard to believe that we are approaching our first anniversary, but it's true. It has been a very interesting endeavor for us, and we hope it has been the same for you. For our anniversary issue, we would like to recognize some of the most unusual CA-related events experienced bu our readers during this past year. So, if you have such a Tale, submit it to us by 19 May. The Editorial Board will vote, and the top two winners will be treated to Anniversary Sundaes by us!

##
NOTE: We MUST receive any submissions for the June issue by 26 May.
##

If you have any comments or suggestions, please submit them to any member of the editorial board.

EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum

[redacted]

OFFICE Reps

[redacted] (b)(3)-P.L. 86-36

[redacted]

[redacted] (b)(3)-P.L. 86-36

\\\

TOP SECRET//COMINT

(C) POC: [redacted] info
(U) Last Modified: 07/24/2006 10:31:51
(U)PE EXTERNAL PAGE

```
**********************************
*        TALES OF THE KRYPT      *
**********************************
```

June 1995

##
//

(FOUO) TABLE OF CONTENTS:

1. CA Perspective from [redacted] D/Chief Z

2. Calendar of Events

3. KRYPTOS News
   a. Norman Roberts Award
   b. KRYPTOS Literature Contest
   c. June Meeting Agenda
   d. Distinguished Members
   e. KRYPTOS Upcoming Elections
   f. [redacted] Chapter News

4. Word from the CACP
   a. Announcements
   b. CA Certifications
   c. CA PQE Results

5. Technical Article - [redacted] on "New Language Model on Westing"

6. Technical Health -
   a. CA-305 Friedman Sessions
   b. [redacted] on "Prescription for Diagnosis"

7. Community Service
   a. MATHFEST '95
   b. Summer Satellite Symposium

8. Problems and Puzzles

##
//

1. (C) PERSPECTIVES IN CA - When "Tales of the Krypt" was first published in June 1994, we asked Tom Lessard to write the inaugural "Perspective in CA". For this anniversary issue we solicited the thoughts of [redacted] Deputy Chief of Z. His topic is...

Future Watch on Cryptanalysis

(b)(3)-P.L. 86-36

(C) Four events in the past few years will have profound impact on the future of cryptanalysis: the apparent end of the Cold War, the decline of Big Government, the worldwide transformation from industrial economies to the information age, and the private sector's recent infatuation with providing information security to an unsuspecting public. One can hardly pick up an Information Age magazine without finding a paragraph in every article explaining the risks and solutions for eavesdroppers, viruses, data integrity, masqueraders, hackers, etc. Formerly the secretive domain of governments, the emerging security provider now more resembles a professor, an engineer, a CIO (Chief Information Officer), a hacker, or perhaps just a "do-gooder". All of these diverse elements have one thing in common: they are primarily interested in securing the global information infrastructure and have little concern or motivation to protect any intelligence.

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

gathering capability. Corporate America is investing big bucks (compared to government) into the R&D for products. Public discussions on vulnerabilities, threats, and the sequence of steps necessary to insure their correction is the everyday chat on the INTERNET. Thus public cryptology has moved from a scholarly interest by the academic community to competition amongst corporations and standards bodies.

(S) So what does all of this mean to cryptanalysis? Are we a dying breed? Certainly not, but we must act quickly to outmaneuver the adversary. The decline of Big Government has already put us on a downward trend just as steep as the increases we saw in the mid-eighties. Of great concern is our inability to hire all kinds of Information Age specialists. In an activity where our people are far more important than any computer or specia-purpose crypto-buster, the only investment of lasting value is indeed our cryptanalytic work force. Our hiring in the mid-eighties formed the core of people who tackled [redacted] and many more. The combination of experienced cryptanalysts and this new breed of mixed cryptanalyst/information technologist was just the formula for the tremendous success we now experience, but it will take super human efforts on the part of us all to sustain the success without the vigorous hiring program we formerly enjoyed.

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) Self-evaluation and self-correction will have to drive a cryptanalytic workforce committed to life ong learning. There is no simple curricula that will be appropriate for everyone. In fact, a diversity of concentrations and interests is far more important than overconcentration on any single-threaded sequence of courses. Much of what any individual must learn will be based on both their own experience and their constantly changing responsibilities in the Information Age. One must find the balance between formal study and surfing professional journals and electronic media.

(U) In summary, I have great expectations for the future of cryptanalytic problem solvers. We have already seen where crypt-analytic training is invaluable to solving many of the non-cipher problems associated with processing. This trend will continue as we confront the full wave of information technology and must rely on creativity and innovation, our real genius, to survive.

.....
//

2. (FOUO) CALENDAR OF EVENTS

June 1	CMI Banquet (BBC, 1830-2300)
June 1	MATHFEST 95 (R & E Symposium Center) (See COMMUNITY SERVICE)
June 5-9	CA-305
June 13-15	Summer Satellite Symposium (see COMMUNITY SERVICE)
June 20	KRYPTOS Talk [redacted] on BULK Encryption, (Friedman, 1315 - new time) (see KRYPTOS SOCIETY NEWS for details)

(b) (3)-P.L. 86-36

PLAN AHEAD

July 7	CMI Talk, David Kahn on "Codebreaking and the Battle of the Atlantic" - (Friedman, 0930)
July 10-14	CA Curriculum Review ([redacted] POC)
mid-October	[redacted]

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

[redacted]

30 Oct - 3 Nov CONSCRYPT

****
//////////

3. (U) KRYPTOS SOCIETY NEWS

a. (S) NORMAN ROBERTS AWARD - CALL FOR NOMINATIONS

In recognition of Norman Roberts' talent for nurturing the skills of junior analysts, the KRYPTOS Society established the Norman Roberts Award. This award may be presented annually to a junior cryptanalyst at NSA/GCHQ who has made an outstanding cryptanalytic contribution.

Norman joined GCHQ in 1975 and won the respect and admiration of his colleagues for his innovative ideas and particularly for his ability to train and inspire younger analysts up to his untimely death in July 1990.

Any KRYPTOS member may nominate any employee at NSA or GCHQ who has approximately five years' service as of 31 July 1995, and who has made an outstanding contribution to cryptology or a related discipline. (For a nominee with more than 5 years of cryptanalytic experience, the citation should explicitly draw the judges' attention to that fact, and explain why the nomination should be considered as falling within the overarching purpose of the Roberts award.) The nominee does not have to be a KRYPTOS member. Integrees will be regarded as members of their host Agency. The nomination must include the names of the proposer and the nominee, together with an account of the work which attracted the nomination. It may be classified up to TSC. Nominations are due by 1 September 1995 and should be mailed to the KRYPTOS Society secretary, [redacted] (b)(3)-P.L. 86-36

The winner, to be chosen by a joint UK/USA panel in October, will receive an engraved plaque and have her/his name inscribed on the permanent Norman Roberts Award plaques displayed at NSA and GCHQ.

****

b. (S) KRYPTOS Cryptanalytic Literature Competition - CALL FOR PAPERS

Sponsored by KRYPTOS, the professional society for cryptanalysts, the competition is open to all personnel at NSA, to personnel on field assignments, and to retirees (consistent with security considerations).

Papers may treat any topic in the broad category of professional cryptanalytic literature, including:
--- attacks and techniques relating to cryptanalytic problems;
--- cryptanalytic research;
--- history of cryptanalysis;
--- other subjects relating directly to cryptanalysis, e.g. target studies, cryptologic trends from the point of view of cryptanalysis, or computer support of a cryptanalytic problem.

Submissions may be written specifically for the competition. They need not be, however. PAPERS WRITTEN BETWEEN JULY 1, 1994 AND JUNE 30, 1995 ARE ELIGIBLE. Entries may carry a classification of up to TSC. Compartmented papers will be considered only in extraordinary cases. Papers should be submitted with one cover sheet with the name(s) and organization(s) of the author(s) and title, and only the title on the papers themselves, to facilitate impartial judging.

The judges will consider the following criteria:
--- Is the paper an original discussion of a cryptanalytic subject?
--- Is the paper well written? Is the subject presented well? Can a reader with a suitable technical background but unfamiliar with the subject understand the paper and, by reading it, gain knowledge about the subject?

(b)(3)-P.L. 86-36

[redacted]

--- Does the paper constitute an important addition to the body of cryptanalytic literature?

The judges will determine up to three winners: cash prizes of $125, $75, and $50 will be awarded to first, second, and third place winners. The judges may designate papers to be worthy of honorable mention. KRYPTOS hopes to publish some of these winning papers in Agency professional journals.

(b)(3)-P.L. 86-36

To enter, please submit four copies of your paper to [redacted] The DEADLINE for entries is JULY 14, 1995. The competition results will be announced at a KRYPTOS function in October 1995.

c. (FOUO) KRYPTOS June Meeting Agenda

1. There will be some limited discussion, then voting, on the Proposed Bylaws changes at the upcoming meeting. These changes will be posted on ENLIGHTEN and to ESS during the first week of June.

2. [redacted] talk is will be on [redacted] Watch ESS and ENLIGHTEN for additional details.

d. (FOUO) Distinguished Members

If you have any suggestions to propose for this year's Distinguished Members, please contact [redacted]

(b)(3)-P.L. 86-36

e. (FOUO) Election Time

Just a notice that this fall is election time for new officers of the KRYPTOS Council. The voting on the proposed changes to the Bylaws at the June meeting will determine just which offices are up for election. If you are interested in running, or would like to suggest someone, please let [redacted] KRYPTOS Secretary, know, either via e-mail [redacted] or by phone; [redacted]

f. ~~(FOUO)~~ [redacted] Chapter News

(b)(3)-P.L. 86-36

The new officers for this chapter took office effective 12 May.

President
President-Elect
Secretary
Treasurer

[redacted]

//

4. ~~(FOUO)~~ CACP NEWS

a. Announcements

1. The CACP is pleased to announce that [redacted] is the new Chairman of the Panel.

2. The CACP also welcomes [redacted] of Z23 as its newest member.

b. CA Certifications

The following people became professionalized in CA during May:

[redacted]

[redacted]

[redacted]

[redacted]

c. CRYPTANALYSIS PQE RESULTS

The 1995 Cryptanalysis Professional Qualification Exam (PQE) was given on 23, 24, and 25 May. Here are a few statistics on this year's offering of the PQE:

(b)(3)-P.L. 86-36

- Of the 24 aspirants who took the exam, 8 passed--and one passed with honors!

- This year's pass rate is the same as it has been in recent years.

- Of those who passed, some had taken the test several times, others had taken it just once before, and still others passed on their first try.

- Among those taking the exam were 6 CA interns, 2 CMPers, and 1 aspirant from the field.

5. (TSC) TECHNICAL ARTICLE

New Language Model Available on Westing [redacted]

WEBMASTERS NOTE: This article has been removed due to classification issues. If you'd like to see the original please contact the current webmaster.

6. (TSC) TECHNICAL HEALTH

a. CA-305 Schedule for Friedman Auditorium

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Monday June 5

1000	Talk 16 #	David Kahn	A New Theory of Intelligence
1230	Talk 12	[redacted]	NSA Overview Briefing
1400	Talk 6 *		The SIGINT Sports Bar: [redacted]

\# - talk is to be broadcast on NEWSMAGAZINE
* - talk is open to NSA and all Second Parties

Tuesday June 6

0830	Talk 33	[redacted]	An Overview of IC-200
1000	Talk 14		NSA/Intelligence Community
1230	Talk 38		Password Cryptography

(b)(3)-P.L. 86-36

[redacted]

1400 Talk 7 + [redacted] Now I Know My A, B , Cs...

+ - talk is open to NSA and UK

Thursday June 8

0830 Talk 8 [redacted] Using the T3D

1000 Talk 11 Why OO in CA Programming?

1230 Talk 22 # Health of US Supercomputing Industry

- talk is open to NSA, IDA, and all Second Parties

Friday June 9

0830 Talk 34 N5 Staff Policy Soup

1000 Talk 34 N5 Staff Policy Soup (continued)

1230 Talk 13 [redacted]

(b) (3)-P.L. 86-36

b. PRESCRIPTION FOR DIAGNOSIS by [redacted]

(C) "What do I do next?" How many of us in the cryptanalytic community have heard this plaintive question from an analyst who had exhausted his/her "bag of tricks" in trying to diagnose a cryptosystem? One of the main issues discussed at the recent cryptanalysis conference at the SRC was diagnosis - what is it, how is it done, what kinds of people CAN do it, can it be taught and, if so, how?

(C) The ability to diagnose cryptosystems was one of the main concerns of [redacted] Chief Z4, as he projected the needs of Z4 into the year 2000. Among his questions were: "How do we train our junior analysts for the challenges ahead? How do we tap the experiences of our senior people before they retire and so learn their "tricks of the trade"? How do we develop the innate diagnostic skills of our analysts? Can we teach creative thinking?"

(C) In an attempt to answer the above questions, in September 1994 a pilot course was developed within Z4 that was designed to sharpen the diagnostic skills of our workforce by exposing them to unusual cryptanalytic problems and then allowing them the opportunity to share with other analysts. From the different divisions in Z4, fourteen analysts of varying degrees of experience in terms of both longevity and exposure were invited to participate in this initial offering. A common alias was established for everyone and the set of problems was placed in a common file. Individuals and small groups were encouraged to work on a particular set of messages, communicating via e-mail on their approaches and results. Then, twice a week we met for an hour for a direct exchange of ideas and "brainstorming". Comments like "I didn't see that" or "I would have never thought of that" were common as each participant began adding to her/his diagnostic repertoire. Unfortunately, other comments like "I didn't have time to work on the problem" also surfaced and pointed out again the need for strong management support for this type of training.

(b) (3)-P.L. 86-36

(C) In November 1994, [redacted] sent me a note asking if this class would be interested in working on some "live" problems. Her branch had isolated some fifteen target systems that were undiagnosed because of low priority and/or lack of diagnostic experience.

[redacted]

Her only request was that the junior analysts in her branch be included in the diagnostic process. What an ideal situation! The analysts in Sylvia's branch worked with a system administrator to set up the various directories and files, and by late November we became a diagnostic exchange group instead of teacher-class. There were no longer any set answers and no "right" way to attack a problem.

(TSC) Since November 1994 the membership in the group has expanded beyond Z4 and is fluid in nature as people with different backgrounds are made aware of the various phenomena existing in these systems and attempt to bring their expertise to bear. We meet once a week for an hour and the agenda varies from the historical to the excitement of a new result. Have we been successful? That depends on what one perceives as the goal. No system has yet been solved. However, in the short time we've been meeting [redacted] One DPP program has been modified and a couple new programs have been suggested. Perhaps the question of success can best be summed up in the comments of [redacted] one of the analysts in [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) "One indicator of the success of this collaboration is the increased confidence demonstrated by some of the junior analysts. They are more willing to discuss their ideas, try new tests, share their results, and trust their own hunches. This gain in self-assurance, coupled with the opportunity to brainstorm with experts, and an expanded "bag of tricks", has led us to characterize this activity as a clear success.

(U) For anyone desiring to join this group and wanting more information about it, feel free to call [redacted] on [redacted] or e-mail [redacted] We try to keep the group reasonably small and would encourage you to join only if you are willing to devote time and effort on the problems.

(b)(3)-P.L. 86-36

....
//////////

7. (TSC) COMMUNITY SERVICE

a. MATHFEST '95

This is a reminder that MATHFEST is coming June 1, 1995, at the R & E Symposium Center. See below for the official schedule. All Green/Gold badgers are welcome, as well as IDA contractors. Talks are limited to [redacted] No special access is required.

There will be a list of abstracts available as a handout at MATHFEST. The CMI is looking to circulate the abstracts throughout the participating offices in advance [redacted] in hardcopy. Be on the lookout for it.

****

M A T H F E S T '95
Schedule of Events

****

0830-0840 Introduction and Welcome [redacted]

Session 1: [redacted] Chairperson

0840-0900 Cryp. App. Prog. Interface-CAPI ([redacted] R21)
0900-0920 [redacted] Z22)
0920-0940 [redacted] Z15)

(b)(3)-P.L. 86-36

[redacted]

Session 2: [redacted] Chairperson

1000-1020 Formal Methods [redacted]
1020-1040 Diagnosis of [redacted]
1040-1100 [redacted] Z52)
1100-1120 [redacted]
[redacted] R51)

Session 3: [redacted] Chairperson

1300-1320 [redacted] Z4)
1320-1340 [redacted]
1340-1400 Automated Signal Identification [redacted]

Session 4: [redacted] Chairperson

1420-1440 [redacted] Z1)
1440-1500 Binary Decision Diagrams [redacted] C7)
1500-1520 [redacted]

Session 5: [redacted] Chairperson

1540-1600 Demodulating Co-Channel V.32 [redacted]
1600-1620 [redacted] (software encryption) [redacted]
1620-1640 [redacted]
[redacted] R51)

(b)(3)-P.L. 86-36

b. Summer Satelite Symposium

Applied Signals Technology is offering this symposium on 13-15 June to "U.S. Government employees". Equipment will be on display in the R&E building lobby; and then four 90-minute seminars will the offered at AST in Jessup on :

Forward Error Correction Code Analysis Processing
Transponder Characterizations and Analysis
Model 120 Users Group
Baseband Channel Analysis

(b)(3)-P.L. 86-36

This is limited to 60 applicants. [redacted] in Z409, has a copy of the registration information and a list of equipment which will be on display. Call her for a hardcopy of the brochure.

8. (~~TSC~~) PROBLEMS AND PUZZLES

a. ANSWER TO FEBRUARY PROBLEM OF THE MONTH

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

all of this sounds far fetched, then I recommend that you attend the CA-305 talk by [redacted] titled "You Can Usually Tell Plain Text, But You Can't Always Tell-a-Cipher". She will describe a real problem that is very similar to this toy. Contact [redacted] for specific details and a diagram of the problem.

****

b. (TOUQ) PUZZLE

1. Answer to the March Puzzle (B-Gone)

H N Y J E
W T R C M
A F O U Q
L X I Z G
S D V P K

(b)(3)-P.L. 86-36

Congrats to the following solvers!

[redacted]

****

c. The New Challenge

Given:

```
   K R Y P T O S
 + S O C I E T Y
---------------
   C P K I I K C
```

Solve for:

0 1 2 3 4 5 6 7 8 9

_ _ _ _ _ _ _ _ _ _

Every letter represents a distinct digit. When the letters are associated with digits so that the addition is correct, they will spell out a phrase that may describe the successful cryptanalyst.

****
//

##
NOTE: We MUST receive any submissions for the July issue by 27 June.
##

If you have any comments or suggestions, please submit them to any member of the editorial board.

(b)(3)-P.L. 86-36

[redacted]

EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, 688-5849

[redacted]

OFFICE Reps

[redacted]

(b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

[redacted]

(b)(3)-P.L. 86-36

TOP SECRET//COMINT

(S) POC: [redacted]
(U) *Last Modified: 10/30/2002 11:42:17*
(U)PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
July 1995

##
//

~~(FOUO)~~ TABLE OF CONTENTS:

1. CA Perspective from David Goldschmidt, CCR-P

2. Calendar of Events

3. KRYPTOS News

4. Word from the CACP

5. Technical Article

6. Community Service

7. Action Line

8. Problems and Puzzles

##
//

1. (~~FOUO~~) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of David Goldschmidt, the Director of IDA-CCR-P, who brings you ...

Greetings from the Center for Communications Research in Princeton.

Many people in the CA-Math community at NSA are acquainted to one degree or another with CCR-Princeton, but I'm sure there are some who have never heard of us, and many others who have only a vague idea of who we are, why we are here, and what we do. So I thought I would take this opportunity (kindly offered by Tales of the Krypt) to tell you something about us, and to try to give you an idea of what things look like from up our way.

We were established in 1959 by recommendation of a high-level committee called the Baker Committee which was established by President Eisenhower to make recommendations about how the United States should develop and expand its cryptologic capabilities. We are a division of IDA, the Institute for Defense Analyses, which is a Federally Funded Research and Development Center with headquarters in Alexandria, VA. We work exclusively for NSA, as do our two newer sister divisions, CCS (formerly SRC) and CCR-La Jolla. There are a number of other IDA divisions located in Alexandria, but they are not involved with NSA at

Approved for Release by NSA on 07-14-2025, FOIA Case # 118218

all.

One of the main thrusts of the original Baker committee report was the idea of strengthening ties between NSA and the outside mathematics community. Back in the fifties at the height of the cold war, NSA was a very ``black'' organization and did not have any of the outside connections which you now enjoy. For many years, the connection with academia was maintained almost exclusively by us, primarily through the SCAMP program which I'm sure many of you have heard of, and quite a few of you have attended. It's an 8-10 week summer program to which we invite roughly 20 outside academics, ranging from bright undergraduates to distinguished senior professors, in addition to colleagues from NSA,

[redacted] (b)(3)-P.L. 86-36

Actually, SCAMP pre-dates the founding of CCR, and almost of NSA itself! The first SCAMP was held at UCLA in the summer of 1952. Its early success was probably at least partly responsible for the Baker committee recommendations. I think it's safe to say that this program has proved over the years to be one of the most successful investments NSA has ever made.

At CCR, our main mission is to develop new cryptanalytic techniques and algorithms, and, more generally, to foster and extend the science of cryptology. Over the years, we've devised many new algorithms, not only in cryptanalysis, but in related fields such as signal processing, language modelling, and speech recognition.

But we don't do this research in a vacuum. Experience has taught us that in cryptology, like any applied science, progress comes from working on hard (even ``intractable'') problems. Trying to solve such problems seems to be the best route to new ideas, algorithms, and techniques which may then apply to many other problems (even if they don't solve the original problem as posed). And every once in a while, we actually do solve the original problem!

Now that I've given you the birds-eye view, let me close with a commercial message. In order to work on real problems, we need close technical researcher-to-researcher contact with NSA. So we have grey phones, we're on the classified network (our e-mail addresses are [redacted] and we have a WWW page [redacted] But even more important, there are in-person visits, both short and long term. We often have an integree in Z Group, and we have a half-dozen or so 1-2 year billets here for NSA integrees. If you're interested in visiting us, either for a short time or a long time, please let me know.

****

//

2. CALENDAR

July 7	Joint CMI/KRYPTOS Talk, "Codebreaking and the Battle of the Atlantic", by David Kahn (Friedman, 0930)	(b)(3)-P.L. 86-36
July 7	Abstracts for CONSCRYPT Due (POC [redacted] Z43, [redacted]	
July 10	Z Tech Forum, "Networking, Now and Tomorrow in Z", by [redacted] and [redacted] J111	(b)(3)-P.L. 86-36

[redacted] (b)(3)-P.L. 86-36

9/23/2010

(b)(3)-P.L. 86-36

(OPS 1, 3SO40, 1300-1400)

July 10-14 CA Curriculum Review [redacted] POC)

July 14 Papers for KRYPTOS Literature Contest Due (POC, [redacted]

July 18 Science and Engineering Society Talk, "How Supercomputers Moved Out of the Basement", by [redacted] 1000)

(b)(3)-P.L. 86-36

PLAN AHEAD

August 17 Joint CMI/KRYPTOS Talk, [redacted] TOPIC TBA, [redacted], 1315)

September 1 Norman Roberts Award Nominations Due

September 15 Peter Jenks Award Nomination Due

mid-October [redacted]

(b)(1)
(b)(3)-P.L. 86-36

October 26 KRYPTOS Annual Banquet and Awards Ceremony

Oct 30 - Nov 3 CONSCRYPT

****
//////////

3. KRYPTOS

a. (FOUO) Amendments to Bylaws Approved

Members of the KRYPTOS Society recently had a chance to vote on some proposed changes to the Bylaws, and the vote was unanimously in favor of accepting these changes. In effect, the terms of office are shortened, creating more frequent opportunities for individuals to offer to serve their community. (A reminder that the Bylaws, with changes annotated, is available on ENLIGHTEN.)

****

(b)(3)-P.L. 86-36

b. (FOUO) KRYPTOS Election News

[redacted] is chairing the Nomination Committee to prepare a slate for the upcoming fall election. She would like to have those KRYPTOS members who might be interested in serving on this committee, or who might be interested in running for an office to contact her, either on [redacted] or [redacted] via e-mail.

(b)(3)-P.L. 86-36

****

c. (FOUO) Peter Jenks Community Service Award

Last year the KRYPTOS Council and the CACP created a new award to recognize an individual for exceptional service and contribution to the CA community. The first recipient was [redacted] Special Assistant to Z5. A detailed description of this award will be available on ENLIGHTEN, and will be mailed to [redacted] Nominations are due to [redacted]

[redacted]

(b)(3)-P.L. 86-36

[redacted] by 15 Sept.

4. NEWS FROM THE CACP (b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

a. ~~(FOUO)~~ CACP Adds New Members

The CACP is pleased to announce the addition of two new members. They are [redacted] Z232, and [redacted] Z0341. They replace [redacted] Z42, and [redacted] Z21. Also, [redacted] has replaced [redacted] on the Computer Program Evaluation Board.

b. ~~(FOUO)~~ NEW FACES IN THE CROWD

The newest CA Intern is [redacted]. He is a recent graduate of University of NC Chapel Hill with a Bachelors Degree in Mathematics. [redacted] was a participant in the UTP. The newest Cross-Trainee, [redacted] will report on 24 July. She was a Resources Manager with a background in Accounting and is returning from Bad Aibling. (b)(3)-P.L. 86-36

c. ~~(FOUO)~~ CA CERTIFICATIONS

The CACP congratulates [redacted] Z53, and [redacted] H111, upon their completion of the CA Professionalization criteria.

d. ~~(FOUO)~~ NEW CRYPTANALYSIS CERTIFICATION CRITERIA

The CACP held an offsite where it considered the recommendations to change the proposed CA professionalization criteria which were made at the CA Conference. Three subcommittees have been formed to investigate retaining the CAPQE in some form, to change the computer program requirement, and to develop the validation requirements for experience and diversity. The recommendations for new courses will be briefed at the CA Curriculum Review. (The CA Curriculum Review will be held during the week of 10 to 14 July.) The Panel will be meeting throughout the month of July to fine tune the plans.

e. ~~(FOUO)~~ HELP WANTED

Look for a job vacancy advertisement in the next HQS booklet for the position of Assistant Executive of the CACP. If you would like to be instrumental in the direction of the CA career field and desire to work with aspirants and interns this may be the position for you. Please call the CACP for more information.

5. (U) TECHNICAL ARTICLE

(b)(3)-P.L. 86-36

ALAS, we have A LACK of technical contributions. Do you want to see your name in a by-line? Is there a particular topic you would like to see covered here? We need support from our readership - soooooo, volunteer to write something, OR, tell us what you want!

****
//////////

6. COMMUNITY SERVICE

a. (FOUO) Nomination Call for First Stephen W. Dilke Crypto-T/A Award

(S) The first Stephen W. Dilke Crypto-T/A Award will be presented at the 1995 Crypto-T/A Conference 17-19 October at GCHQ. This award recognizes any CANUKUS individual or group who has used crypto-T/A to make a significant contribution to SIGINT. The Stephen W. Dilke Award may be given across CANUKUS Agencies (i.e. CSE, GCHQ, NSA), Groups/Division and career fields since the key determining factor is the use of crypto-T/A in intelligence. As successful crypto-T/A is typically a group effort, it will not be unusual for more than one person to receive the award. An inter-agency committee of representatives at GCHQ will select this year's winner(s). It is anticipated that the Agency hosting each year's Crypto-T/A Conference will convene a similar committee to select that year's Dilke Award winner(s).

(S) Nominations may come from anyone and should include the name, e-mail address and secure telephone number of the person making the nomination. Information about the nominee should include a writeup of the contribution, explaining each person's role and the SIGINT benefit that resulted. This year's nominations should be forwarded to:

[redacted] (b)(3)-P.L. 86-36

[redacted] is ready to provide further advice on the process to anyone at NSA who would like to submit a nomination(s). The deadline for nominations is COB 31 July 1995.

****
//////////

b. (FOUO) Newsletter Needs a New Office Rep

We have an opening for a Z3 rep on the editorial board, as [redacted] is moving on. If you are interested, please let us know.

****
//////////

7. ACTION LINE:

a. (FOUO) QUESTION: Knowing that I am in Z Group, a friend of mine in another Group stopped me in the hall the other day and asked my opinion on a situation. She wanted to know if a student at Anne Arundel Community College (who works in Z Group) can write a paper on encrypting email for class. I told her that as long as the information used in the paper came from open source (and there is a lot of open source on that topic), I did not see a problem. She then told me that

(b)(3)-P.L. 86-36

[redacted]

the person had used FOUO documents and told the teacher that he could see the references used in writing the paper but that he (teacher) could not keep them. That part of the story changed my view. I don't think that FOUO information should be used in a school paper. Would you please give me an official reading on this?

A Z Manager (b)(3)-P.L. 86-36

****

ANSWER: (Provided by [redacted] Z CAO)

Dear Z Manager,

FOR OFFICIAL USE ONLY is UNCLASSIFIED information that is protectable (withheld from the public) under the Freedom of Information Act (FOIA) and Public Law 86-36. FOUO information may be disseminated within the US Government, contractors, consultants and guarantees to conduct official business. Holders of FOUO information are authorized to convey this information to officials within the government to conduct official business.

The long and short of this is that FOUO information may not be taken out of this building for personal use without the signed permission of N5. An example might be a chapter out of the PMM one might need. If an individual wanted to use information in a school paper, it should have been taken to N5, who would redact the (FOUO) information. An example of that would be an individual's name, organization, or SSN.

There has been quite a bit published in policy.online about this subject; but, we will continue to bring this subject to people's attention, either in classification.online or in Znotes. A lot of times people will read something, and think that the article was not meant for them. So, if anyone needs clarification on any classification issue, such as this, please feel free to discuss it with me.

****

b. (~~FOUO~~) QUESTION: We have heard that the DO is requiring Tech Track membership as a prequisite for promotion for all people in technical fields. Is this true?

(b)(3)-P.L. 86-36

****

ANSWER: (Provided by [redacted] for the DO)

The DDO's policy is that as a rule, for promotion to GG/14 and GG/15, a person in the technical field should have at least applied for a title.

****

//

8. PUZZLES AND PROBLEMS

a. (~~FOUO~~) Answer to Last Month's Puzzle

The following people forwarded the correct answers to last month's puzzle:

(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

[redacted]

b. (FOUO) This Month's Challenge [redacted] our new Puzzle Editor)

The following groups of letters represent anagrams of nine common 4-letter words. Anagram them, and then change the first letter in each one to form a new word. Choose the nine new letters so that they spell out (in order) yet another word. What is it?

EMAT
TNHU
ATHE
OBRE
CSAE
RILA
THBA
ESHO
AVSE

(b)(3)-P.L. 86-36

Send your answer to [redacted] at [redacted] and we will publish the list of correct solvers in the next issue.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

c. (TSC) PROBLEM OF THE MONTH

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

NOTE: We MUST receive any submissions for the August issue by 26 July.

If you have any comments or suggestions, please submit them to any member of the editorial board.

(b)(3)-P.L. 86-36

EDITORIAL BOARD

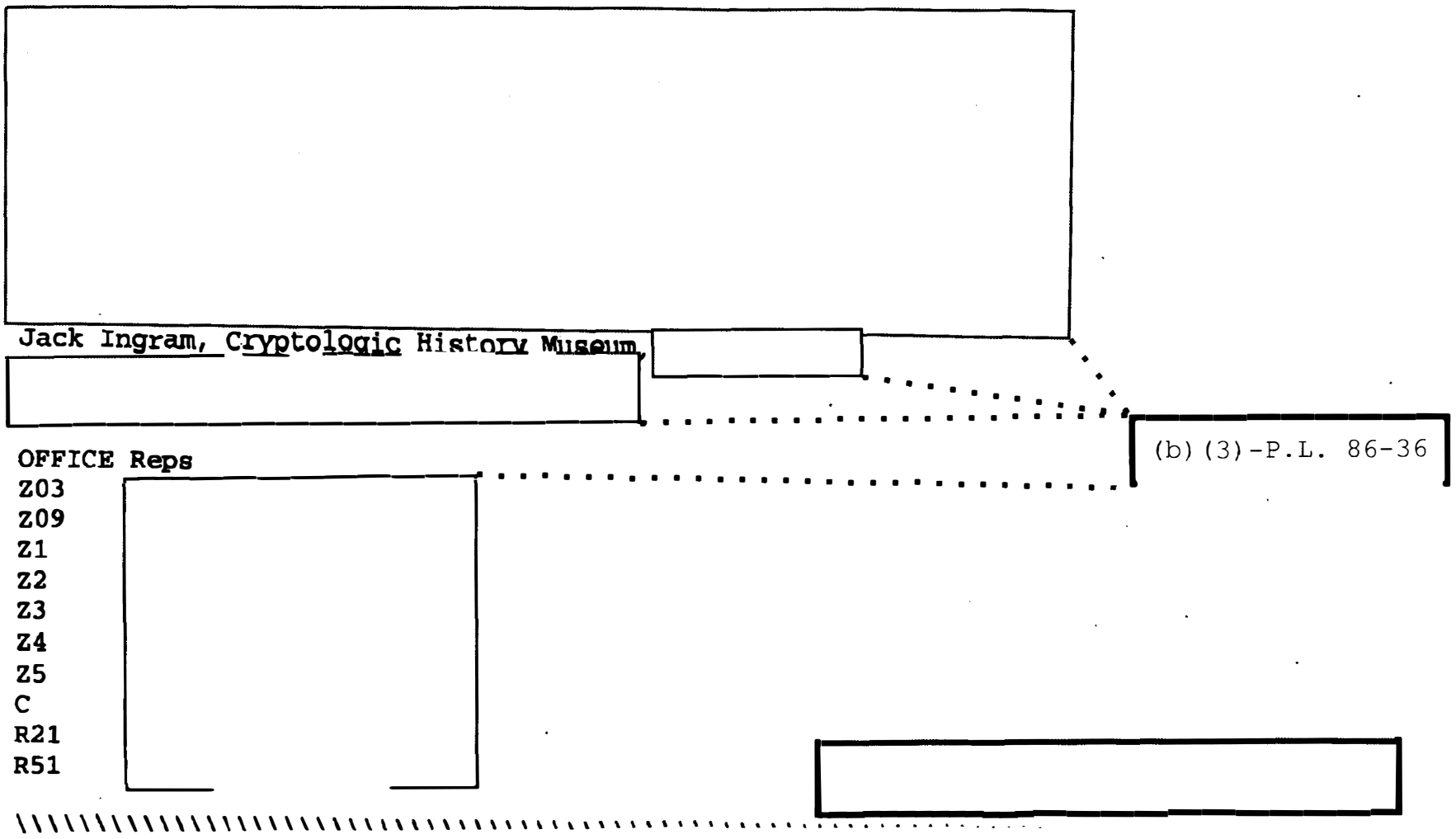
[redacted]

[redacted]

9/23/2010

July 1995 TALES OF THE KRYPT

Doc ID: 6892732 Doc Ref ID: A3863379



TOP SECRET//COMINT

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:17
(U)PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
August 1995

//

(FOUO) TABLE OF CONTENTS:

1. CA Perspective from [redacted] Chief, Z3
2. Calendar of Events
3. KRYPTOS News
4. Word from the CACP
5. Technical Article
6. Community Service
7. Historic Tidbits
8. Problems and Puzzles

(b)(3)-P.L. 86-36

//

1. (FOUO) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of [redacted] Chief, Z3.

(b)(3)-P.L. 86-36

WE ARE OUR FUTURE

(C-CCO) As I think about the future of cryptanalysis, I find my crystal ball is very imprecise, but yet I know WE will continue to be extraordinarily successful. WE have been responsible for our success in the past, and WE will be responsible for our success in the future. Through OUR very hard work, our capabilities really do keep up with our target's capabilities.

(S-CCO) We have made unimaginable strides over the decades, yet we also have much in common with our predecessors. The commonality with our past is what gives me confidence in our future. We have always had wonderful people, working on beautiful problems, using super technology. We often hear that cryptanalysis is our core discipline, and it is. But the important fact is that WE ARE CRYPTANALYSIS today, WE have been in the past, and WE will be in the future. I include all of Z in this WE along with our colleagues elsewhere in NSA (primarily in the DT and INFOSEC organizations), in IDA, in our 2nd (and in a few cases 3rd) party partners, and in some less commonly recognized intelligence and law enforcement agencies. To be successful, CA must be an inclusive discipline, not an exclusive club. Our job is difficult, and we must be open to innovative approaches to doing our

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

job. I believe our predecessors did that, and succeeded. They taught us that with our PEOPLE, and determination we could do the impossible. We continue to do the impossible today.

(~~FOUO~~) We cannot take future success for granted. I don't know where the future will take us, but I know with certainty how we will get there. WE will get there through the skills of our people. It sure helps to have good problems to push us to new heights, but the overriding factor is US (that means YOU and ME). And, the key to OUR success is our TECHNICAL HEALTH. Technical health is no accident. The first intern programs and professional societies were in the CA field. The CA field has been the leader in continuing education. But, we cannot rest. The world and our problems are changing rapidly, and we know we must change with them. We must each take responsibility for our continued growth. The technology we will be using ten years from now and the targets we will be exploiting will be vastly different from today. We cannot afford to let either the technology or the targets leave any of us behind. If we become complacent, we will lose. We must not only learn new "facts," but new ways of working together. Teamwork and collaboration must really become part of our routine way of operating.

(~~FOUO~~) WE really are wonderful people, WE ARE OUR FUTURE, I do have confidence in US, and that is why CA will continue to be successful.

****

//////////

2. (~~FOUO~~) CALENDAR

August 3 — R51 Seminar - "A Cryptomathematician's View [redacted] R51 Math Lab, Rm R1S048) (See Aug. 10th)

August 3-4 — NSA Software Reuse Symposium (R&E Symposium Center)

August 8-10 — INFOSEC Research and Technology Transfer Conference (TECHFEST) - Sponsored by R2 - (Maritime Institute - POCs, [redacted] or [redacted])

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

August 10 — R51 Seminar - "A Cryptomathematician's View [redacted] R51 Math Lab, Rm R1S048)

August 17 — Joint CMI/KRYPTOS Talk, [redacted] "The Day of the Dodo, Some Escapades from the Past" (Friedman, 1315)

August 25 — Views on Professionalization; A Personal Story by [redacted] Technical Advisor to Chief Z. (0900-1100, 9A135)

(b)(3)-P.L. 86-36

PLAN AHEAD

September 1 — Norman Roberts Award Nominations Due (Send to [redacted])

[redacted]

September 15	Peter Jenks Award Nominations Due (Send to [redacted]
mid-October	[redacted]
October 26	KRYPTOS Annual Banquet and Awards Ceremony
Oct 30 - Nov 3	CONSCRYPT (FANX)

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

3. (U) KRYPTOS NEWS

a. (~~FOUO~~) Nominating Committee to Meet

It is time to think about the election of KRYTPOS Officers for next year, and the Nominating Committee, chaired by [redacted], is looking for volunteers. If you are interested in hearing more about which offices will be available, please contact Joan.

4. (U) WORD FROM THE CACP

a. (~~FOUO~~) New Certifications Announced

At the 14 July meeting the CACP presented Letters of Certification to [redacted]

b. (~~FOUO~~) GOLD BUG Team Award Announced

DDO will present the Gold Bug Team Award to [redacted] on 9 August.

(b)(3)-P.L. 86-36

c. (~~FOUO~~) Job Opportunity

The Job Vacancy Announcement for the Assistant Executive positions (95HQS598) will close on 18 August. For additional information, contact either [redacted].

d. (~~FOUO~~) Interview of New Cross-Trainee, by [redacted]

(U) [redacted] has been a cryptanalysis cross-trainee since April and she "loves it". She has always had an interest in cryptanalysis and was delighted to be selected for the program.

(b)(3)-P.L. 86-36
(b)(6)

[redacted]

(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36
(b)(6)

e. (FOUO) Books Needed

The CACP is in need of Military Cryptanalytics I, II, and III for those individuals who are new to the career field. If you have any not in use, please forward them to the Career Panel Office. If you would like to obtain a copy, please call the Panel Office.

5. (U) TECHNICAL ARTICLE

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(TS//CCO) The [redacted] Tutorials [redacted]

(U) We're learning to do things differently these days which means we have to be smarter about so many things. Some obstacles are obvious: if there's no TDY money, you don't go. You coordinate a little better, work a little smarter and somehow manage to get the job done. Other obstacles aren't so easy to see, which makes their impact a little more difficult to measure. One of those intangibles is the loss of corporate knowledge we suffer every time a colleague of long-standing departs.

[redacted]

(b)(3)-P.L. 86-36

(FOUO) Do you really have to wait for your resident guru to tell you how to run a particular program, or work a new system?

(FOUO) [redacted] is making headway in its effort to capture some of that knowledge and make it available to everyone who needs it [redacted]

[redacted]

(U) The [redacted] lessons take advantage of the best features of "Pop-Up Prompt" (PUP) tutorials and advance a step further. Through creative use of hypertext links, [redacted] allows you to go after only the information you want, without wading through pages of material.

(U) The nature of the lessons also lend themselves to easy updates. Should something change or if there's a better way to convey a message, it can be done on the spot.

[redacted]

[redacted]

software should consider providing an accompanying tutorial 'de rigueur'. It is proving to be a very effective piece of documentation to provide to users.

(U) To add further versatility, we're in the midst of moving to hypertext mark-up language (HTML) for WWW browser viewing. Not only does the medium itself allow for easier movement among the documents, but it will allow easier access to the tutorials than what the Frame Maker version permits. We think you'll be pleased with the change.

(U) If you have material--notes, manuals, ANYTHING--you think would be beneficial to others, please let us know. We'll work with you to whip it into shape and make it a viable lesson.

(U) Finally, we actively solicit your feedback on the lessons already published. Did we capture the essence of the program? Could we have said it better? Did we say too much? Too little? Those of you learning to use a new program are in the best position to tell us how valuable our tutorial was to you.

(U) We're on the web:

[redacted] (b)(3)-P.L. 86-36

takes you to the [redacted] Home Page. You'll find set up instructions and a "point and click" menu that will take you where you need to go.

********** Here's what's on line **********

[redacted] (b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

(TOUO) DIAGNOSTIC PROGRAM PACKAGE (DPP) Tutorial
(It's in both FrameMaker and HTML formats)

(TOUO) [redacted] TOOLBOX For the [redacted] Databases (b)(3)-P.L. 86-36

**********And under construction (but available for review) *****

[redacted]

[redacted]

6. (U) COMMUNITY SERVICE

a. (U) The Z Technical Library now has various articles on Women in Mathematics, Science and various other professional fields. Request copies of articles from [redacted], Z Technical Librarian, or if you have any new articles to add to the collection, please send the them to her, attention-Z509, Headquarters Building.

b. (U) Cryptologic History On-Line

(FOUO) The Center for Cryptologic History, E322, invites all Agency personnel to subscribe to its history categories on the Electronic Subscription Service (ESS) and ENLIGHTEN. Two or three times a week the Center publishes "CRYPTOLOGIC ALMANAC," a gallimaufry of historical notes about our cryptologic heritage. Sometimes these notes are pegged to an important anniversary, sometimes they just recount an interesting and instructive incident from the past.

(FOUO) The Center also uses these categories to announce its new publications, provide the work force with information about the annual history symposium, and disseminate news about new exhibits or activities at the National Cryptologic Museum. E322 is also pleased that many Agency employees use these categories to provide feedback about the Center's activities.

(FOUO) The ESS topic number is 1364. The ENLIGHTEN newsgroup is pubs.hist. If you have general questions on the Center for Cryptologic History, please contact Dave Hatch on [redacted] for questions on the Center's publications, contact [redacted] on [redacted]

(b)(3)-P.L. 86-36

c. (U) Write Line [redacted]

The Write Line, a service manned by the faculty of the Intelligence Production Work Center at the NCS, is set up to answer questions on grammar, punctuation, word use, and anything else you can talk them into! Over the course of the 10 plus years that Write Line has been in existence, the faculty has answered questions from almost every organization in the Agency, ranging from "Is there a comma before 'and' in a list?" to "What is the accepted abbreviation for 'Chief' in an MR? The Write Line number is not in the phone book, but they do give it out freely - [redacted].

d. (FOUO) New Pers Rep

M3Z is pleased to announce that [redacted] returning from [redacted] is now assigned as a Pers Rep. The distribution of accounts will now be:

[redacted]

(b)(3)-P.L. 86-36

[redacted]

A reminder: they are located in Room 2N018, and can be reached on 3036s.

****

e. (FOUO) Access you Personnel Profile (Provided by M3Z)

To check up on your personnel profile, simply send e-mail to perinfo@nsa with a subject line of profile. The text of the message should contain only your social security number without any dashes, i.e., 123456789. You will receive back a listing of your personal stats, test scores, classes, past performance appraisals, awards, and previous positions held.

****
//

7. (U) HISTORICAL CA PERSPECTIVE

a. (TSC) Extract from CRYPTOLOGIC ALMANAC - The Story of VENONA

(U) On 11 July NSA declassified the existence of VENONA--the cryptanalytic effort against the communications of the KGB's predecessor organization and GRU. The VENONA effort encompassed 2,200 messages; on 11 July NSA released forty-nine messages and pledged to release the balance over the next year.

(U) Until recently, the word VENONA loomed large for only a small segment of the Allied intelligence and counterintelligence community. Now, VENONA may well become as famous as the terms PURPLE, MAGIC, ENIGMA, and ULTRA. And just as those well-known catchwords for American and British cryptanalytic successes of World War II conjure up their war-shortening code and cipher breaking achievements against the military forces of Nazi Germany and Imperial Japan, so too will VENONA become the byword for the postwar American and British cryptanalytic successes against a collection of high-level encrypted Soviet intelligence service communications. The seemingly miraculous (but actually tireless and skillful) code breaking of the VENONA traffic helped the FBI expose dozens of Soviet KGB and GRU agents and their traitorous American collaborators in the U.S., including the atomic spies Julius and Ethel Rosenberg.

(S) As with almost everything cryptologic, describing the VENONA project is complicated. Soviet diplomatic communications, essentially telegrams between Moscow and its embassies and consulates abroad, contained the traffic that became known as VENONA. [redacted] Analysis initially determined that five systems and subscribers were involved: Trade, Diplomatic, KGB, GRU and GRU-Naval. The KGB system contained the bulk of readable traffic of intelligence and counterintelligence value in the VENONA program.

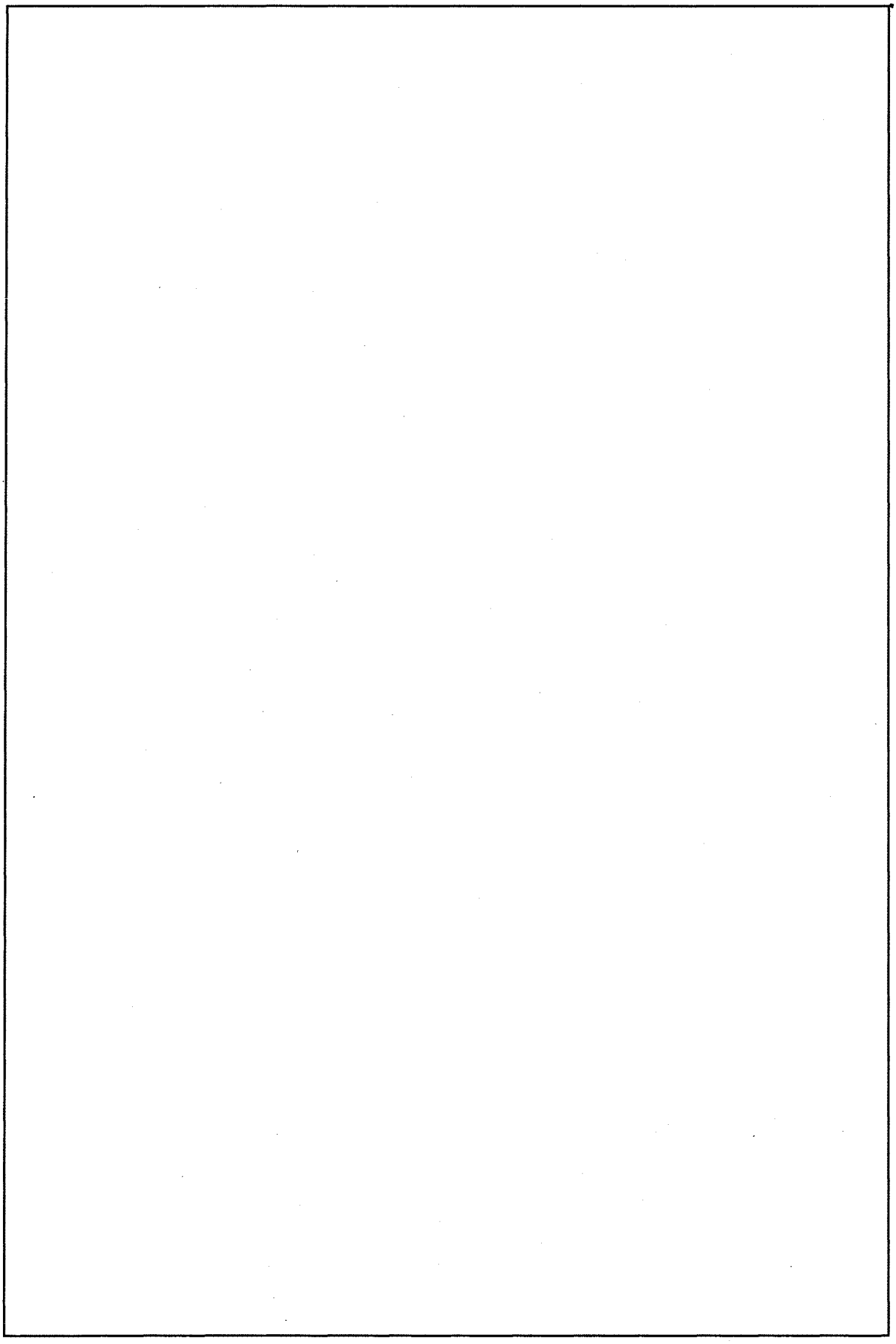
(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(TSC) But all these systems and subscribers contributed to the phenomenon that made some of the traffic readable. [redacted]

[redacted]

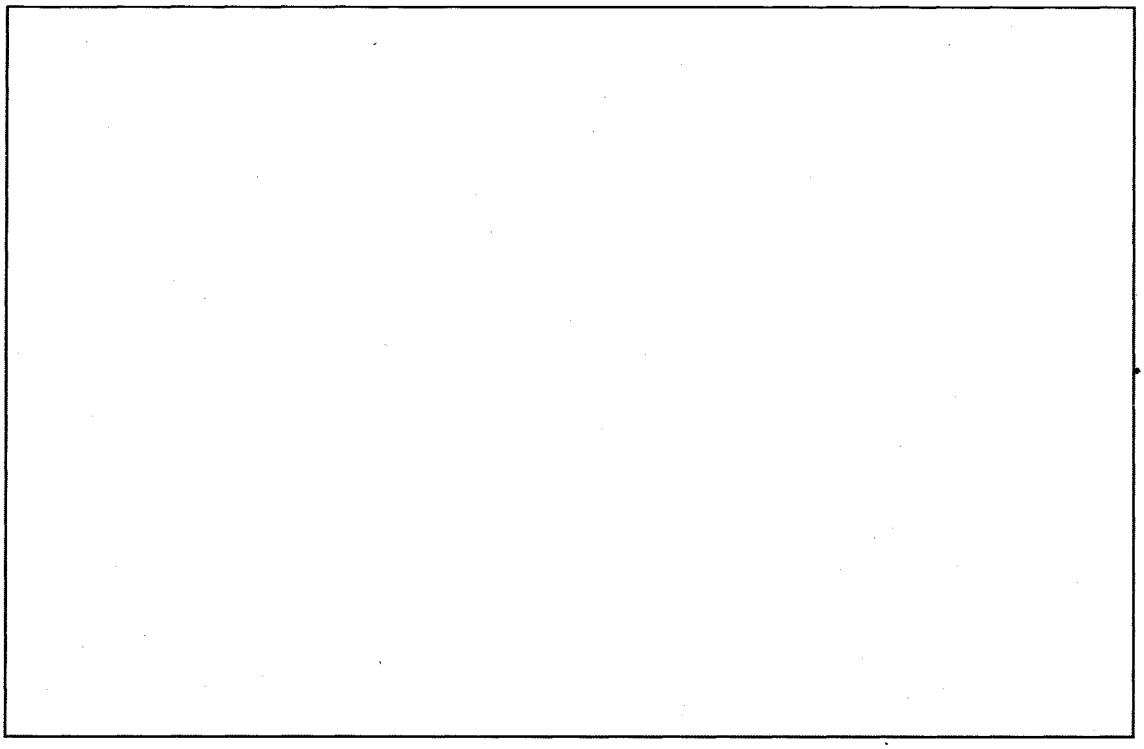
(b) (3)-P.L. 86-36

[redacted]



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) That's enough for now. This is intended as the first in a series of "Cryptologic Almanac" items designed to introduce the VENONA effort to a wider Agency audience. It is important history that can now be told. Over 100 Americans were identified by name in and through VENONA as agents of Soviet intelligence, and another 100 probable but unnamed Americans were known to be agents and informants. They worked in the 1940s for the State Department, Treasury, Justice, the OSS, the military, the Manhattan Project, even the White House and Congress, to name a few federal government organizations. The VENONA codebreaks were of enormous value in helping uncover and end the espionage efforts of many of these Soviet spies in the early days of the Cold War.

[Based on materials contained in the _History of VENONA_ by Robert Louis Benson and Cecil James Phillips, in three volumes, National Security Agency, 1995 (TSC).]

[Michael L. Peterson, Center for Cryptologic History, E322, [redacted] or [redacted]]

8. (U) PUZZLES and PROBLEMS OF THE MONTH

(FOUO) We will begin to alternate monthly between Problems of the Month and Puzzles, so in effect everyone will have two months to solve each and have his/her name appear in the newsletter. Therefore, readers have another month to solve [redacted] last Problem.

(b)(3)-P.L. 86-36

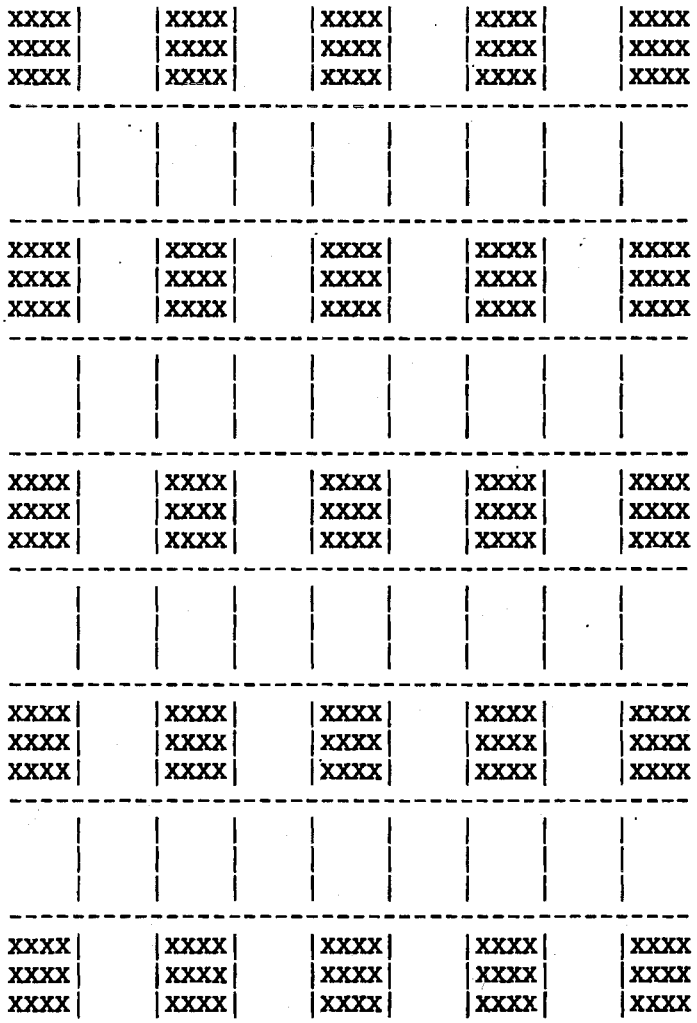
a. (FOUO) The following people correctly solved last month's puzzle -

[redacted]

[redacted]

b. ~~(FOUO)~~ August Puzzle [redacted] (b)(3)-P.L. 86-36

The clues below refer to the following grid. Since the clues are unnumbered, finding out where the answers go is up to you. The clues are cryptic, i.e. similar to crossword puzzles found in England. The basic idea behind cryptic clues is that half the clue is a straight definition, and the other half of the clue is a play on words.



Generically European articles, coming and going, surround unfinished poem (9)
Striking notes lead confused civet (9)
Product of mixed marriage brought about by edges of halters offcast, up to a point (5-4)
Man takes a tablet in hairlike item (9)
Inflammation of a vein sounds like bugs catching little one (9)
Pike's arty negotiations provide ballplayers salary? (6,3)
Innocent untruths confuse the 51 wise (5,4)
Dog leads quiet jerk backing up on most of Ten Square (9)

Have fun!

[redacted] (b)(3)-P.L. 86-36

***

Doc ID: 6823798

TOP SECRET//COMINT

(S) POC: [redacted] info

(U) Last Modified: 10/30/2002 11:42:18

(U)PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****

September 1995

(b)(3)-P.L. 86-36

//

(FOUO) TABLE OF CONTENTS:

1. CA Perspective

2. Calendar of Events

3. KRYPTOS News

4. Word from the CACP

5. Technical Corner

6. Community Service

7. Historic Tidbits

8. Problems and Puzzles

//

1. (FOUO) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of Jeff Zehe, Chief C1.

~~~~~~

(b)(3)-P.L. 86-36

(U) When [redacted] asked me to write an article several months ago, my immediate thought was to write about the new C Group - how we have been reengineered - what's our new game plan and how does it mesh with NSA's Core Process Team actions including the soon to be published NSA Corporate Plan for INFOSEC. Although there's so much more I'd like to know and understand before I write this note, there have been a lot of developments. I also want to seize the opportunity to tell you a little about a new initiative called the Crypto Mathematics Education Board.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted] (b)(3)-P.L. 86-36
~~~~~~

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

In INFOSEC, the old ground rule was "the adversary knows all there is to know about your system"; the new ground rule is "the adversary is a member of your net". Our interests are even more intertwined than before...INFOSEC's challenges are SIGINT's opportunities / SIGINT's challenges are INFOSEC's opportunities...perhaps even on the same network.

(SC) There are several factors that have driven the C reorganization.

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(FOUO)~~ The Crypto Math Education Board (CMEB) was established last fall (under the Mathematics Carrer Panel) to care for the cryptomath curriculum at the National Cryptologic School. We (1) recruit, facilitate training for and support instructors, (2) monitor and develop the curriculum to satisfy community needs, and (3) provide a reliable interface between the School and the community. Since September 1994, we have met every three weeks. In addition to helping [redacted] recruit instructors, we have worked on developing the curriculum. We've continued [redacted] effort to improve CA-235, discussed MA-246 with former instructors to identify measures to improve and update this course, and laid out the foundation for a telecommunications sub-curriculum. [redacted] is revising MA-145/146 and new public key/number theory courses are in design. Members of the CMEB are [redacted] and Jeff Zehe. We are acting for you; we want your input and may seek your support.

(b)(3)-P.L. 86-36

2. ~~(FOUO)~~ CALENDAR

September 8	Norman Roberts Award Nominations Due (Send to [redacted])
September 8	CMI Presentation [redacted] CCS (Friedman, 0930)
September 14	Science and Engineering Society Presentation, [redacted] R52/W9W (1000, R&E Symposium Center) (See 6b)
September 15	Peter Jenks Award Nominations Due (Send to [redacted])
September 22	CA Technical Track Ceremony (9A135, 1300)

(b)(3)-P.L. 86-36

PLAN AHEAD

October 6	CMI Talk - Topic to be Announced (Friedman, 0930)
October 10	OKTOBERFEST, a joint KRYPTOS/CMI Gala (Last Chance, Columbia) (see 3a, below)

[redacted]

Doc ID: 6823798

October 17-19	Cryptanalytic Computing Conference (See 6d)
mid-October	[redacted] (b)(1) (b)(3)-P.L. 86-36
October 26	KRYPTOS Annual Banquet and Awards Ceremony
Oct 30 - Nov 3	CONSCRYPT (FANX)

//

//

3. KRYPTOS

a. (~~FOUO~~) Second Joint KRYPTOS/CMI After-Hours Celebration Scheduled

The next Kryptos/CMI party is planned for Tuesday October 10th from 5:30 to 7:30 at the Last Chance in Columbia. As we did at the last party, we will be collecting $5.00 per person to cover the cost of appetizers. The cost of drinks will be the responsibility of each attendee. (But please order from the waiters/waitresses instead of at the bar so we get credit for the order.) We will begin taking reservations and money around the middle of September. POCs: [redacted] More info later.

//

4. CACP NEWS

a. (U) ISDP

Most people are aware of the Intern and Cross Training Programs administered by the Cryptanalysis Career Panel (CACP), but there is a lesser known program that is also in existence. It is the Individual Skills Diversification Program, or ISDP. This program can fill many purposes. It can be used by the professionalized cryptanalyst wishing to update his/her CA skills, by someone in a related field wishing to acquire some CA skills, or by someone in the CA field who lacks some of the requirements toward certification.

In the ISDP, the Career Panel acts in an advisory capacity. The participant is not detailed to the CACP, but remains on his/her own billet. This requires the support and commitment of the participant's organization. The ISDP participant will, in conjunction with the CACP, draw up a plan or roadmap to get him to the goal. This may involve a list of diversity assignments, courses, or other activities. Next the participant gets the concurrence of his management, and then, remaining on his billet, goes on a mini, self-styled intern program.

The program benefits the individual by improving his technical skills and knowledge; it benefits the host organization because they get back a more well-rounded analyst; and it benefits the organizations providing the diversity because they get "free help" in the form of a person loaned to them with a billet.

If you would like more details on how this program can work for you, contact the CA Career Panel office on [redacted]

(b)(3)-P.L. 86-36

[redacted]

b. ~~(FOUO)~~ CACP TIDBITS

1. In July there was a curriculum review for Cryptanalysis. Testimony was heard from instructors, and information gathered from people who had taken CA courses and their supervisors. A panel headed by Tom Lessard, Chief Z, took all the information into account and came up with some recommendations for improving the CA curriculum. The report from the Cryptanalysis Curriculum Review Board is almost complete, and will be available on MOSAIC in the near future. For additional information, contact [redacted] Z09.

2. The 1995 Cryptanalysis Conference Report, CA-2000, was mailed out to all conference participants and Z offices this month. If you would like a copy, contact the CA Career Panel office. Also, newly revised tech track criteria for cryptanalysis are available by contacting the CA Career Panel office.

3. If you have any suggestions for how to improve the Technical Track, contact [redacted]. She is part of a DO THAB subcommittee that is studying the results of the recent tech track survey and suggesting ways to improve the Agency's Technical Track program.

4. There will be a ceremony to confer titles on recent members of the CA Technical Track, to be held on 22 September at 1300 hours in room 9A135. A reception will follow the ceremony. If you are interested in attending, please contact the CA Career Panel office on [redacted]

(b)(3)-P.L. 86-36

c. ~~(FOUO)~~ CA COURSE DESIGNATORS CHANGED

Beginning in FY-96 there will be some changes in course designators:

CA-112 will become CA-212
CA-101 will become CA-202

//

5. TECHNICAL CORNER

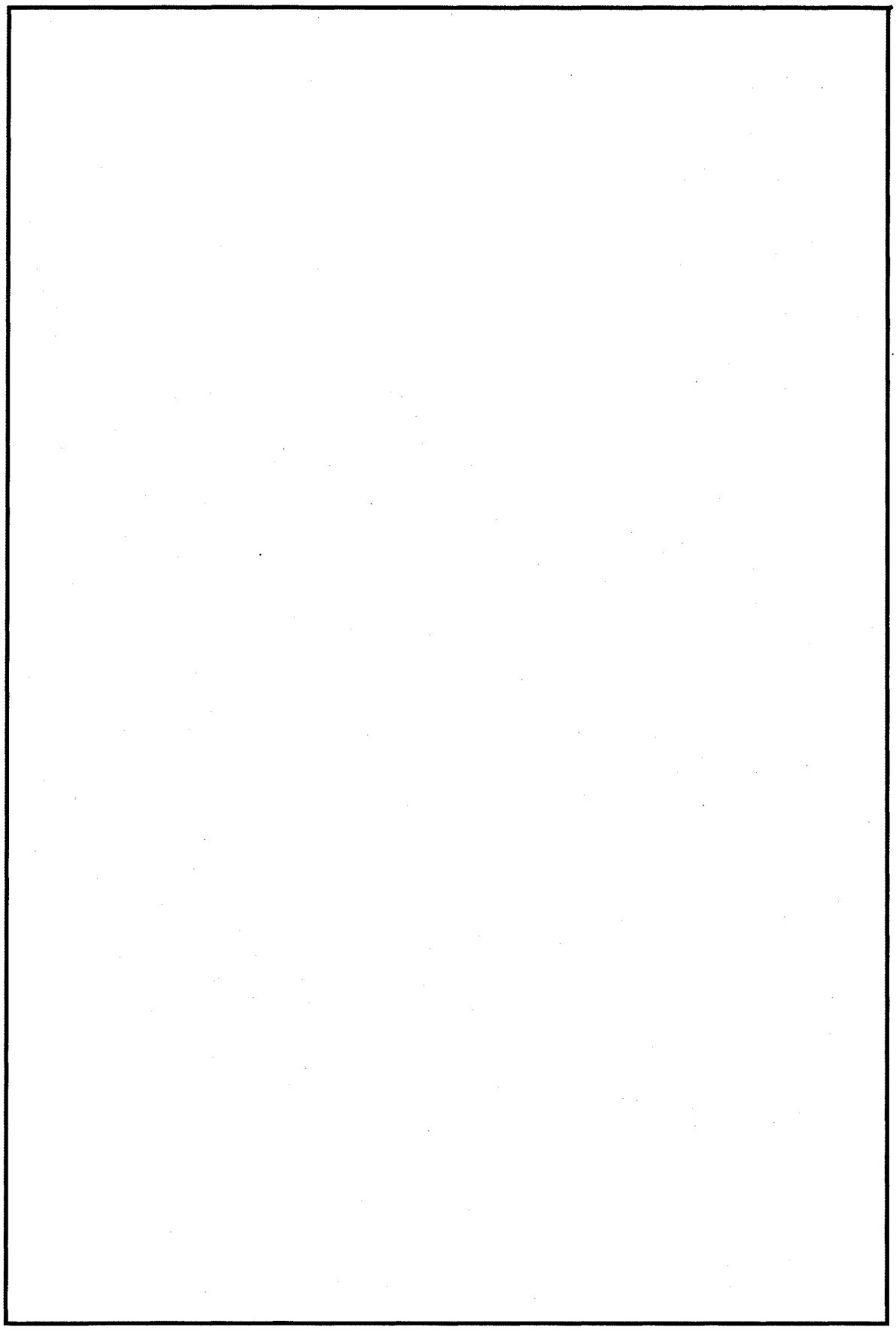
a. ~~(TSC)~~ [redacted] in a Nutshell [redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

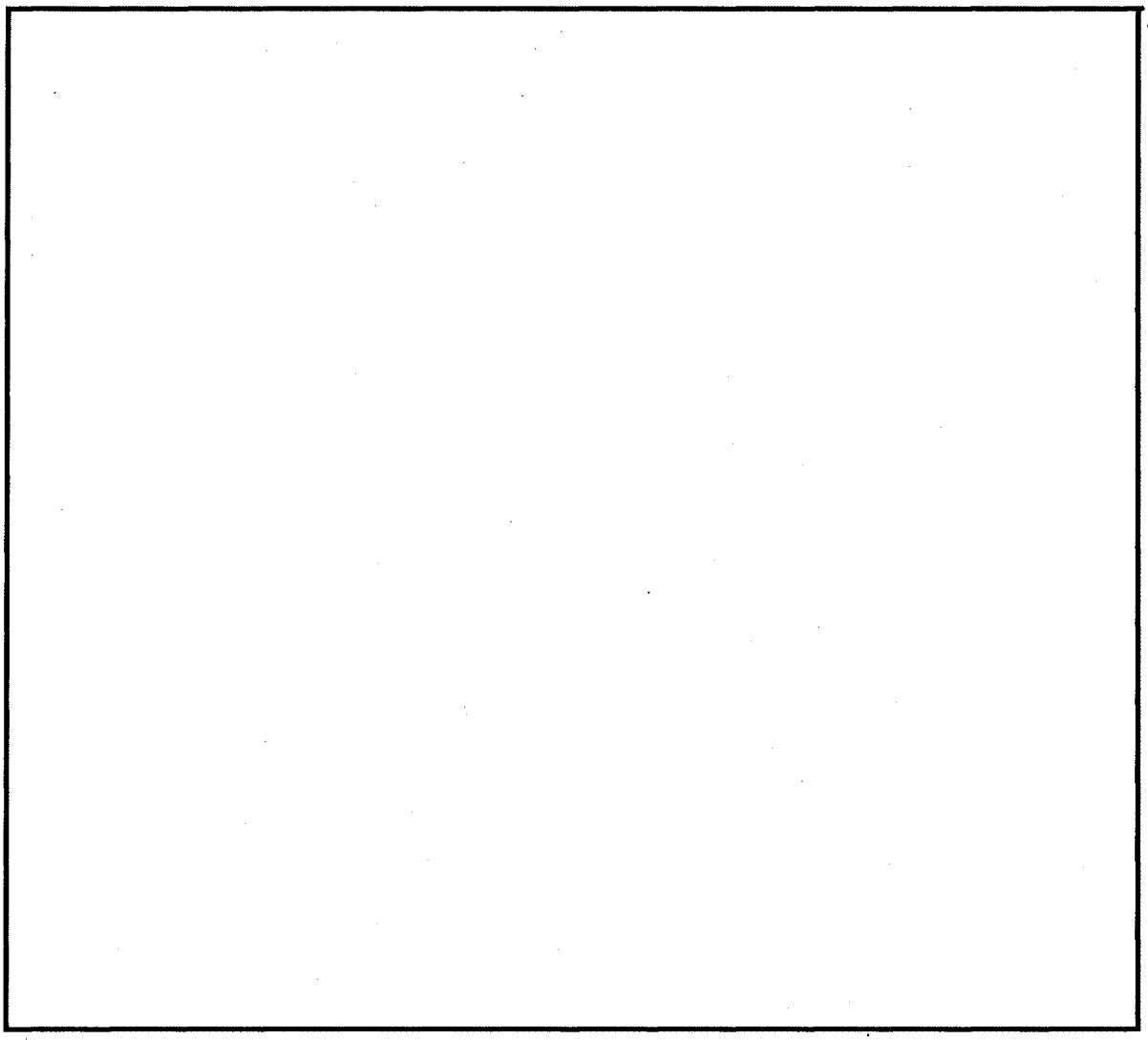
[redacted]

(b)(3)-P.L. 86-36



(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

b. ~~(FOUO)~~ Tech Trend Note

(The following was exacted from this quarterly periodical published by the [redacted] on C4I technologies of interest to the Information System Security Organization. For further information or suggestions please contact: [redacted]

(b)(3)-P.L. 86-36

QUANTUM CRYPTOGRAPHY-BASED SECURE KEY DISTRIBUTION done for the first time over long distances. Achieved on a 10km optical fiber circuit at BT Labs in the UK, the process encodes key on pairs of quantum effects that, according to fundamental physical laws given in Heisenberg's uncertainty principle, cannot be observed without changing the key and thus alerting legitimate users to the intrusion. The work shows it is possible to build a practical quantum-based system of key distribution. (Electronics Letters Vol 30, No.10 via Proquest. See also Scientific American Oct92)

[redacted]

//

6. COMMUNITY SERVICE

a. ~~(TSC)~~ Fourth Annual Cryptanalytic Computing Conference

The Cryptanalytic Computing Conference (C3) is a forum for presenting recent work on the computational aspects of cryptanalysis. Major topics include:

+ Applications and Algorithms - practice and experience
  algorithm design and analysis, data structures, innovative mappings of problems to parallel and vector architectures, techniques influenced by new architectures, comparative performance studies, software and hardware reverse engineering

+ Computing Tools for Cryptanalysis
  languages and compilers, distributed job management, production control systems, software development environments

+ Architectures for Cryptanalysis (proposed and in use)
  SPD's, ASICS, workstation accelerators, high-speed networking, etc.

The conference will be held October 17-19, 1995 at the Center for Computing Sciences in Bowie, Maryland.

Information for Attendees

A (classified) copy of the conference program can be obtained via electronic mail (see below). If you would like to register for the conference (and have a folder prepared for you), contact [redacted] at the address below. Attendees without NSA green badges should determine if they have current TSSI clearances on file at the Center for Computing Sciences (CCS); ask your Cognizant Security Authority or call the number provided below. Those attendees without current clearances (or NSA green badges) should arrange to have their clearances forwarded to the CCS Security Manager well in advance of the conference. Attendees with NSA green badges are not required to have clearance documents at CCS.

(b)(3)-P.L. 86-36

Please submit your conference registration request no later than September 22.

Conference Chair:

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

****

b. ~~(TSC)~~ Science and Engineering Society Presentation

[redacted]

[redacted]

(b)(3)-P.L. 86-36

Doc ID: 6823798

[redacted] during an NSA - sponsored fellowship. He has been with the Agency for fifteen years, mostly in W group. He has degrees in physics and mathematics and has played par golf once.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

For information on or membership in the Society contact:
Tom Kline [redacted]

***

FORMAT - written; 120 unclassified multiple choice questions.

LOCATION - TBA; either the Ops1 or Ops2A/2B cafeteria.

MISCELLANEOUS - Open to all green/gold/black badgers.
- Those who helped draft the questions are eligible to participate, but cannot receive the cash prizes.
- To preregister, send a note to [redacted] by COB 11 Sept.

e-mail: [redacted]
phone:
office:

(b)(3)-P.L. 86-36

****
//////////

7. ~~(FOUO)~~ HISTORIC TIDBITS

This month we feature a series of monographs written in 1966 by Lambros Callimahos. They not only illustrate his keen grasp of technical concepts and an uncommon attention to detail, but also show a side to the great analyst that unfortunately only a handful of today's NSA family have had the opportunity to experience firsthand.

==========

Monograph No. 1.

FOREWORD

This publication heralds the first in what is hoped will be a series of definitive treatments of important topics facing the scientist in this technological age. Although this first monograph is hardly controversial in its nature or approach, it nevertheless faces squarely up to a rather sticky problem that has long baffled, puzzled, rankled, and bothered mathematicians all over the free world. Like Euler's Identity and Gauss's formula for the number of primes under N, the utter simplicity of this presentation should appeal to both novice and expert alike, requiring as it does only the rudiments of counting, although graduate study in celestial mechanics is certainly not a bar to its full appreciation.

I wish to thank the Directors of the Ptolemy Club Research Foundation for their encouragement in the face of adversity, and for the insubstantial grant which made this far-reaching study possible. I also wish to acknowledge the assistance of my good wife, Helen, who egged me on and on and on; not only did she read through the manuscript, but she gave me her unstinting help and unflagging cooperation without which this work no doubt could not have seen the light of no day. Any errors in this paper are the author's, of course. Comments, criticisms, and suggestions for revision are invited.

/s/ Lambros D. Callimahos
Washington D.C.
11 February 1966

==========
==========

(b)(3)-P.L. 86-36

[redacted]

Doc ID: 6823798

A Short Table of Even Primes

2

Monograph No. 2.

FOREWORD

The widespread interest and universal acclaim greeting the publication of Monograph No. 1 in this series of definitive treatments of important topics facing the scientist in this technological age is heart-warming indeed, right through the left auricular cockles. This present paper goes directly to the stomach of a problem which patently has been unclear for generations; otherwise, why hasn't it appeared in print before this? Why, why, why -- the burning question hammers at the top of the scientist's head. Now, for the first time, and in clear, unambiguous exposition, we have the value of unity expressed to 1600 decimals, which should be enough for the average engineer's uses, if not precise enough for the astrophysicist.

I wish to thank the Directors of the Ptolemy Club Research Foundation
.....
Comments, criticisms, and suggestions for revision are invited.

/s/ Lambros D. Callimahos
Washington D.C.
12 February 1966

Unity Expressed to 800 Decimal Places

1.00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000 00000 00000

(b)(3)-P.L. 86-36

9/23/2010

Doc ID: 6823798

Monograph No. 3

FOREWORD

The furor created in the scientific world in the last two days, following the appearance of Monographs Nos. 1 and 2 in this series, was beyond our wildest expectations. Congratulatory telegrams have been coming in diurnally from Hoboken, New Jersey to Addis Ababa. (Actually, they were all sent from Hoboken, New Jersey, to Addis Ababa by mistake.) This present paper, another triumphal first, gives the first 200 integral powers of 1. The calculations were effected by using Napier's bones. (The bones were on loan from the British Museum, through the courtesy of the Napier family.) Calculation was complicated owing to the absence of the right femur, with subsequent round-off error.

I wish to thank the Directors of the Ptolemy Club Research Foundation
.....
Comments, criticisms, and suggestions for revision are invited.

/s/ Lambros D. Callimahos
Washington D.C.
13 February 1966

==========

Powers of 1, from 1 to 1 (1 200)

Exp.	P	Exp.	P	Exp.	P	Exp.	P	Exp.	P
1	1	41	1	81	1	121	1	161	1
2	1	42	1	82	1	122	1	162	1
3	1	43	1	83	1	123	1	163	1
4	1	44	1	84	1	124	1	164	1
5	1	45	1	85	1	125	1	165	1
6	1	46	1	86	1	126	1	166	1
7	1	47	1	87	1	127	1	167	1
8	1	48	1	88	1	128	1	168	1
9	1	49	1	89	1	129	1	169	1
10	1	50	1	90	1	130	1	170	1
11	1	51	1	91	1	131	1	171	1
12	1	52	1	92	1	132	1	172	1
13	1	53	1	93	1	133	1	173	1
14	1	54	1	94	1	134	1	174	1
15	1	55	1	95	1	135	1	175	1
16	1	56	1	96	1	136	1	176	1
17	1	57	1	97	1	137	1	177	1
18	1	58	1	98	1	138	1	178	1
19	1	59	1	99	1	139	1	179	1
20	1	60	1	100	1	140	1	180	1
21	1	61	1	101	1	141	1	181	1
22	1	62	1	102	1	142	1	182	1
23	1	63	1	103	1	143	1	183	1
24	1	64	1	104	1	144	1	184	1
25	1	65	1	105	1	145	1	185	1
26	1	66	1	106	1	146	1	186	1

(b)(3)-P.L. 86-36

9/23/2010

Doc ID: 6823798

27	1	67	1	107	1	147	1	187	1
28	1	68	1	108	1	148	1	188	1
29	1	69	1	109	1	149	1	189	1
30	1	70	1	110	1	150	1	190	1
31	1	71	1	111	1	151	1	191	1
32	1	72	1	112	1	152	1	192	1
33	1	73	1	113	1	153	1	193	1
34	1	74	1	114	1	154	1	194	1
35	1	75	1	115	1	155	1	195	1
36	1	76	1	116	1	156	1	196	1
37	1	77	1	117	1	157	1	197	1
38	1	78	1	118	1	158	1	198	1
39	1	79	1	119	1	159	1	199	1
40	1	80	1	120	1	160	1	200	1

==========
==========

Monograph No. 4

FOREWORD

By this time, the whole world knows that the Ptolemy Club Research Foundation Monograph Series is to be reckoned with. (We pause for a few milliseconds to let that one sink in.) As an adjunct to computation, the Monographs are truly sine-qua-nonical, absolutely nonpareil, and very useful to boot. Most texts give implicit values of quantities raised to the zero power; but now, for the first time in history, we have an _explicit_ listing of 120 quantities raised to this power. In addition -- and this may not occur to the average reader, this Table also contains a handy listing of the squares of numbers from 1 to 120. The proper use of _any_ mathematical table should embrace an adequate understanding of its component parts.

I wish to thank the Directors of the Ptolemy Club Research Foundation
.....
Comments, criticisms, and suggestions for revision are invited.

/s/ Lambros D. Callimahos
Washington D.C.
14 February 1966

Table of $(N^2)^0$ for 120 Integral values of N

N	N^2	$(N^2)^0$	N	N^2	$(N^2)^0$	N	N^2	$(N^2)^0$
1	1	1	41	1681	1	81	6561	1
2	4	1	42	1764	1	82	6724	1
3	9	1	43	1849	1	83	6889	1
4	16	1	44	1936	1	84	7056	1
5	25	1	45	2025	1	85	7225	1
6	36	1	46	2116	1	86	7396	1
7	49	1	47	2209	1	87	7569	1
8	64	1	48	2304	1	88	7744	1
9	81	1	49	2401	1	89	7921	1
10	100	1	50	2500	1	90	8100	1
11	121	1	51	2601	1	91	8281	1
12	144	1	52	2704	1	92	8464	1

(b)(3)-P.L. 86-36

9/23/2010

Doc ID: 6823798

13	169	1	53	2809	1	93	8649	1
14	196	1	54	2916	1	94	8836	1
15	225	1	55	3025	1	95	9025	1
16	256	1	56	3136	1	96	9216	1
17	289	1	57	3249	1	97	9409	1
18	324	1	58	3364	1	98	9604	1
19	361	1	59	3481	1	99	9801	1
20	400	1	60	3600	1	100	10000	1
21	441	1	61	3721	1	101	10201	1
22	484	1	62	3844	1	102	10404	1
23	529	1	63	3969	1	103	10609	1
24	576	1	64	4096	1	104	10816	1
25	625	1	65	4225	1	105	11025	1
26	676	1	66	4356	1	106	11236	1
27	729	1	67	4489	1	107	11449	1
28	784	1	68	4624	1	108	11664	1
29	841	1	69	4761	1	109	11881	1
30	900	1	70	4900	1	110	12100	1
31	961	1	71	5041	1	111	12321	1
32	1024	1	72	5184	1	112	12544	1
33	1089	1	73	5329	1	113	12769	1
34	1156	1	74	5476	1	114	12996	1
35	1225	1	75	5625	1	115	13225	1
36	1296	1	76	5776	1	116	13456	1
37	1369	1	77	5929	1	117	13689	1
38	1444	1	78	6084	1	118	13924	1
39	1521	1	79	6241	1	119	14161	1
40	1600	1	80	6400	1	120	14400	1

==========

==========

Monograph No. 5

FOREWORD

To coin a phrase -- we being numismatic Pharisees from way back -- "Necessity is the mother of invention." The giraffe grew a long neck to reach the tops of trees, and early Eiderdown man developed ten fingers to match his decimal counting system. Mapier, Burgi, and Briggs compiled logarithmic tables to three different bases, all unusable by extraterrestrials with only 3 1/7 fingers. Striking a blow for interplanetary amity, this brilliantly conceived table will win for us new friends in our Galaxy -- and God knows we could use some. For the pi-fingered gentry, these logarithms will be viewed as a good boon, even from the point of view of a Cyclops with an orb perched on top of his main universal joint.

I wish to thank the Directors of the Ptolemy Club Research Foundation

.....

Comments, criticisms, and suggestions for revision are invited.

/s/ Lambros D. Callimahos
Washington D.C.
15 February 1966

==========++++++++++==========

==========

(b)(3)-P.L. 86-36

9/23/2010

Abridged Table of Logarithms to the Base Pi

("Lambrosian Logs")

N	Logarithm
1	0.0000
2	0.6055
3	0.9597
4	1.2110
5	1.4060
6	1.5652
7	1.6999
8	1.8165
9	1.9194
10	2.0115

==========

==========

Monograph No. 6

FOREWORD

Accustomed as we are to burning questions -- carminatives will often help -- we are totally unprepared for the untenebrific, unfrigorific reception accorded the publication of these papers. In brief, the rhapsodic lillibullero after each paper, starting with the distant rumblings reminiscent of eerie viscera and swelling to a Walpurgis crescendo of incredulous unbelief, punctuated by a myriad nan oboes inflected in agonized tones rising along an exponential curve to a shocking 2000-cycle note beyond the wildest lamentations of the fair lady of Lammermoor -- such is the warp (and woof) of the Monographs. Now that we are exhausted, consider this present paper as having an adequate introduction.

I wish to thank the Directors of the Ptolemy Club Research Foundation

.....

Comments, criticisms, and suggestions for revision are invited.

/s/ Lambros D. Callimahos
Washington D.C.
16 February 1966

==========

The Last 24 Positive Integers, in the Arab World

24
23
22
21
20
19
18
17
16
15
14

. . . . (b)(3)-P.L. 86-36

13
12
11
10
9
8
7
6
5
4
3
2
1

==========

==========

Monograph No. 7

FOREWORD

This present Monograph is a fitting tribute to the culmination of seven days of feverish activity on our part. It will mark the last Monograph in the series, since the Board of Directors of the Ptolemy Club Reasearch Foundation have seen fit to utilize our multifaceted talents for the relief of human misery, not for creating additional problems. We were quite flattered at the first kudo (sic): captaincy in the Salvation Army, politely declined. The second kudo (sic sic): Director of the Pakistani Planned Parenthood Association, declined as being unprolific. The third offer was accepted with alacrity (Alacrity is a Greek friend of ours): Chamber Virtuoso of the Lion of Judah, an imposing title, pregnant with possibilities.

I wish to thank the Directors of the Ptolemy Club Research Foundation
.....
Comments, criticisms, and suggestions for revision are invited.

/s/ Lambros D. Callimahos
Washington D.C.
17 February 1966

==========

The 100,000th Decimal Digit of Pi,
after the Decimal Point

5, uh, 6, er, 5, no wait, 6 ...

****

8. (U) PUZZLES and PROBLEMS OF THE MONTH

~~(FOUO)~~ We will begin to alternate monthly between Problems of the Month and Puzzles, so in effect everyone will have two months to solve each and have his/her name appear in the newsletter.

****

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

a. (FOUO) The following people correctly solved last month's problem -

[redacted]

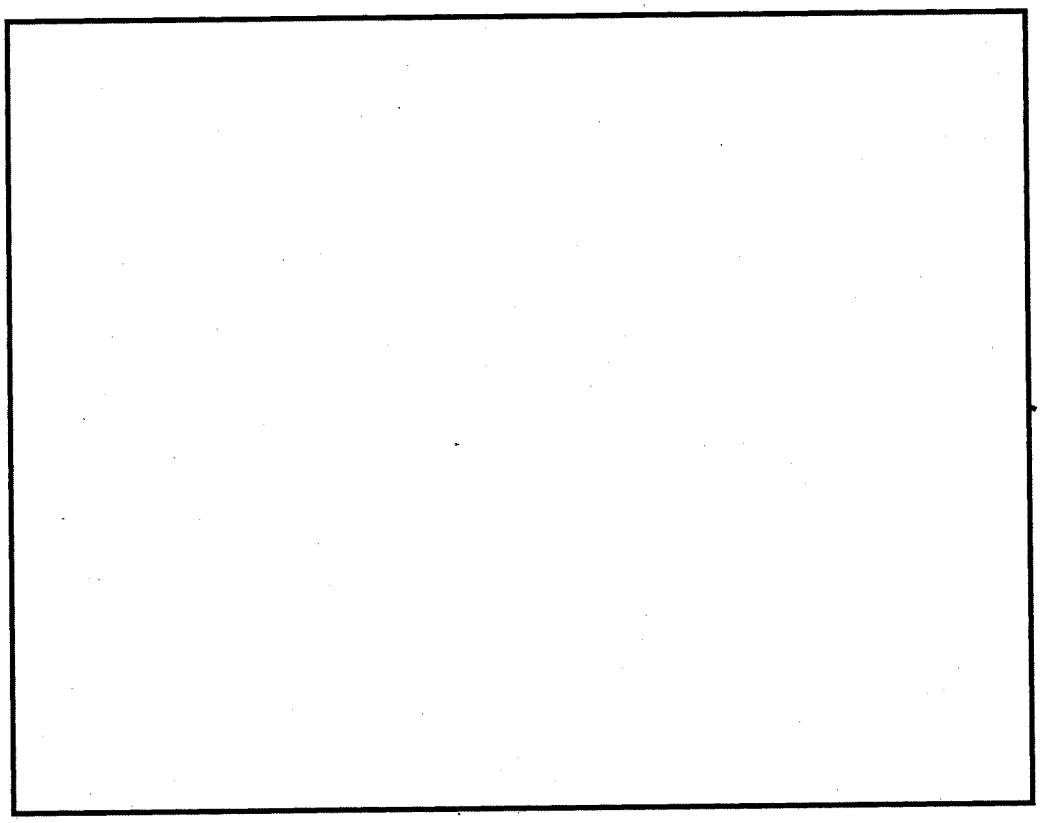
As you may recall, the problem was a putative plaintext message from a real problem. [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

[redacted]



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

b. PUZZLES

Correct answers from the last puzzle were submitted by [redacted] Congrats to them.

1. The following puzzle is courtesy of [redacted] (b)(3)-P.L. 86-36

The commonest way to write out a list of words is alphabetically. This may be all that is needed in many circumstances, but it can have unfortunate side effects (nods from those whose last name starts X, Y or Z). So the following 19 words have been deliberately written in a "fairer" order.

BALLAD ACHING LEDGER ITALIC ADSORB BILLET USABLE RICHER TERMED KERNEL
LESSEE MANTRA ENSIGN SONATA PELMET ENTRAP OREGON CERVIX PORTAL

Problem 1. Identify the method used to order the list of words.

Problem 2. Rearrange the list of 19 words, so they are in the "correct" order. (Puzzle solvers are left to decide for themselves what "correct" really means, and may submit either this new ordering, or the algorithm used to generate it).

Problem 3. Explain the significance of 594 - (this provides a check on the "correct" solution to Problem 2).

2. (U) And Another One .....

We received another submission, this one from [redacted] who found it in Martin Gardner's "Codes Ciphers and Secret Writings", (b)(3)-P.L. 86-36

[redacted]

published by Simon and Schuster , New York, 1972. (The original is a hand-written graphic depiction of symbols, which we have tried to represent as closely as possible from the keyboard. For a copy of the original, contact [redacted] (b)(3)-P.L. 86-36

A CRYPTO-RIDDLE: What goes "zzub, zzub, zzub"?
(The cryptogram below contains the answer.)

! `66 H/FU\^

`!%*@!#-

****

(Our Puzzle Editor would like to encourage anyone who has a puzzle he/she would like to submit to send it to him. Thanks!)

****
//////////

##########

NOTE: We MUST receive submissions for the October issue by 27 September.

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

[redacted] (b)(3)-P.L. 86-36

[redacted]

TOP SECRET//COMINT

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:18
(U)PE EXTERNAL PAGE

[redacted] (b)(3)-P.L. 86-36

****
* TALES OF THE KRYPT *
****
October 1995

//

(FOUO) TABLE OF CONTENTS:

1. CA Perspective

2. Calendar of Events

3. KRYPTOS News

4. Word from the CACP

5. Technical Corner

6. Community Service

7. Problems and Puzzles

//

1. (FOUO) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of [redacted] Chief Z31.

[redacted] (b)(3)-P.L. 86-36

(S-CCO) A Military Standard

(C-CCO) There are days when the negatives seem to outweigh the positives; days when furlough talk permeates the air, and you wonder if you're "essential"; days when you learn that the decrypts you're sweating to produce fall "below the reportable threshold"; days when the bureaucracy does something objectionable (well, that's every day so it doesn't matter!). I've learned in recent years to put a lot of this in a much better perspective by focusing on one thing: our core mission, support to military operations. I'd like to share this perspective as my tale.

(C-CCO) I'm not a rabid militarist, far from it, but I do see this part of our job as particularly clear and compelling, revitalizing because it is so real and immediate. My awareness of this is recent, developing over the short time I've enjoyed as Chief of Z31, which is supporting military operations somewhere in the world pretty much every day.

(FOUO) First, no matter how anxious the military situation, no matter how serious we all are as we try to succeed, this is satisfying, enjoyable work. I say "enjoyable" intentionally, even though we may be talking life and death. People have a goal and commit heart and soul

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

to achieve it. They inevitably look back on their efforts with fond memories. This is something to remember when the next furlough or downsizing rumor comes around, suggesting that we are expendable in some sense. If you've just helped keep soldiers out of harm's way, you have no inner doubts about the value of your contribution.

~~(FOUO)~~ Second, people work together without constraint. Teamwork and efficiency predominate. Information gets to those who need it, computer resources are assembled and connected overnight, mathematicians and signals converters find common ground. All the petty stuff that inhibits cooperation vanishes without trace.

~~(S-CCO)~~ Third, bureaucracy melts away when military operations come up. [redacted] Other offices can top that, I'm sure. Office, Group, Key Component boundaries are immediately transparent. Money is found when it's clearly needed. I have the dubious distinction to be the Cryptanalysis category manager as well as Chief Z31, meaning I lead formulation, presentation and defense of our budget. Cryptanalytic support to military operations is a briefing show-stopper, without fail. Cryptanalysis, the Agency's core discipline, is seen to be prosecuting the Agency's core mission, and it deserves and gets the support it needs.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TS-CCO)~~ Now, I don't want anyone who isn't working military support at this moment to feel maligned or neglected by this. I realize that we can't give every problem the same priority as the [redacted] much less the Gulf War. I know research doesn't work quite this way. And I know that there are many cryptanalytic work centers, with no military support role, but where cryptanalysts make extremely valuable contributions to our Agency's mission, enjoy their work, have a strong sense of mission, work well with others, and do not feel unduly constrained by bureaucracy and resource shortfalls.

~~(C-CCO)~~ But I also know that this level of satisfaction and productivity is hard to maintain when the latest memo comes around encouraging everyone to retire or prepare for a furlough. For me, our history of success supporting the military, and the way we do that, provides an inspirational standard to compare with what I am doing today, a principle that says do what needs to be done to reach your objective, no matter what gets in the way. That principle applies to anything we do. It helps me forget about the irritations of the moment. It is something we have to do much more consistently in a future which consists of a smaller organization and a much more challenging target environment.

****
//////////

(b) (6)
(b) (7) (C)
OGA

2. ~~(FOUO)~~ CALENDAR

FBI

October 3	Science and Engineering Society Presentation, "Applying Technology to Apprehend and Convict", by [redacted] Special Agent of the FBI, (R&E Symposium Center, 1000) (see beloq)
October 6	CMI Talk - Topic to be Announced (Friedman, 0930)
October 10	OKTOBERFEST, a joint KRYPTOS/CMI Gala

(b) (3)-P.L. 86-36

[redacted]

	(Last Chance, Oakland Mills Village, Center, Columbia 1730-1930)
October 10	Z Tech Forum, "Opportunities in Network Analysis", [redacted] (3S040, OPS1, 1300) (b)(3)-P.L. 86-36
October 12	DDO Tech Track Masters Ceremony
October 17-19	Cryptanalytic Computing Conference (C3) (CCS) (see 6a, below)
October 16-20	[redacted] (b)(1) (b)(3)-P.L. 86-36
October 26	KRYPTOS Annual Banquet and Awards Ceremony
October 27	Z/H Offsite
Oct 30 - Nov 1	Third Annual Computer Communications Conference (Friedman - Keynote Speaker, William Crowell, D/Dir, Oct 30th, 1300)
Oct 30 - Nov 3	CONSCRYPT (FANX)

Plan Ahead

November 17	KRYPTOS Talk (TBA) and General Election (Friedman, 1300)

3. (U) KRYPTOS

a. ~~(FOUO)~~ DISTINGUISHED MEMBERS ANNOUNCED (b)(6)

The KRYPTOS Council is delighted to announce the names of those recently chosen as Distinguished Members, [redacted] all former NSAers. These gentlemen will be formally inducted as Distinguished Members at the Annual Luncheon to be held on October 26th at the Fort Meade Officers' Club. The winners of the Literature Contest and the recipients of the Norman Roberts Award and the Peter Jenks Community Service Award will be announced as well. To sign up for the luncheon, contact [redacted]

b. ~~(FOUO)~~ LAST CHANCE (b)(3)-P.L. 86-36

Just a reminder that the Joint KRYTPOS/CMI Octoberfest will be held at the Last Chance at the Oakland Mills Village Center in Columbia on Tuesday the 10th of October from 5:30 to 7:30 p.m. A mere $5 per person includes a variety of appetizers including Potato Skins, Buffalo Wings, Beer Battered Mushrooms, French Fries, Buffalo Meatballs, Nacho Grandes, Cheese Quesadillas, and Garlic Bread au Gratin! Drinks are extra. Contact any of the following to sign up and pay. We need to have a head count by October 5th.

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted] (b)(3)-P.L. 86-36

4. (U) CACP NEWS

a. ~~(FOUO)~~ MONTHLY MYSTERY ANALYSTS - THEN AND NOW

Each month the CA Career Panel office will feature, on its third floor bulletin board, a new cast of mystery analysts. At the beginning of the month we will display photos of the analysts earlier in their careers. As the month progresses, clues to the identities of the analysts will appear. If you think you can guess the identity of one or more of the featured analysts, e-mail your guesses to h111@nsa. People guessing correctly, as well as the names of the mystery analysts, will be published in the following month's edition of the Tales of the Krypt.

(Note: the CA bulletin board is located in the 3rd floor breezeway between the OPS 1 and HQS buildings.)

==========

b. ~~(FOUO)~~ CA-2000 UPDATE

~~(FOUO)~~ Since the CA conference in March, the Career Panel has been working to refine and incorporate the recommendations in the conference report into a new plan for CA professionalization. Subcommittees have been formed to study various aspects of the criteria, and the panel hopes to be able to publish some new guidelines by the end of the year. A current status report of how things are looking as of 1 October is included below.

~~(FOUO)~~ The six major areas of certification will remain, but may change form somewhat. These areas are:

1. Experience: requirement will remain the same, but the method of validation (currently the PERSUM) will change.
2. Diversity: will be restructured to include 3 core areas and 2 specialty areas. Method of validation will also be altered.
3. Training: several new courses are to be developed (this requirement will probably change the most). The career panel is working with the newly formed CA Education Board on recommendations from the 1995 curriculum review.
4. PQE: there will still be a PQE, but the format will probably change - maybe several times. The eventual goal is to automate it so that canned software can be used in solving the problems.
5. Paper: the requirement for a technical paper will remain

[redacted] (b)(3)-P.L. 86-36

unchanged.

6. Program: there will still be a programming requirement, but some modifications will be made in what is accepted. This should result in a "relaxing" of some of the topics and languages that are acceptable.

(U) As a reminder, this is still a draft, and none of these changes have been officially approved or put into effect yet.

==========

c. ~~(TOUO)~~ NEW CA CAREER PANEL STAFF

The Cryptanalysis Career Panel (CACP) welcomes the following new members to the team:

[redacted] formerly of Z42, will be replacing [redacted] as Assistant Executive.

[redacted] formerly of Z21, will be the new Administrative Assistant for the Career Panel.

[redacted] Executive of the Systems Acquisition Management Career Panel (and former CA intern), will be helping out the CA panel with various activities.

[redacted] (Z32) is the new Engineering Advisor, and [redacted] (Z21) is the new Mathematics Advisor to the CACP. The Advisor positions (a Computer Science Advisor will be named shortly) have been created to assist the panel in drafting new criteria for certification as CA moves to include more Math, Engineering, and Computer Science, and as a resource for interns, cross-trainees, and aspirants with those technical backgrounds who may want advice on courses to take or tours in their specialty area.

[redacted] (Z233) has replaced [redacted] on the Computer Program Evaluation Board.

Teresa Levendusky (Z232) will replace [redacted] on the Technical Paper Evaluation Board.

(b)(3)-P.L. 86-36

==========

d. ~~(TOUO)~~ NEW CRYPTANALYSTS ON THE LOOSE!

Four "future cryppies" joined H111 this month:

CA Cross Training Program:

[redacted]

CA Intern Program:

[redacted]

We welcome them to our career field!

(b)(3)-P.L. 86-36

==========

e. ~~(TOUO)~~ CONGRATULATIONS

[redacted]

The Cryptanalysis Career Panel is pleased to announce the promotion of recently graduated intern [redacted] now in Z211, to GGD-13.

[redacted] CA intern, received an SPCA from the CACP for work done on the DPP while assigned to Z443 for his first tour.

[redacted] of Z223 received TWO cash awards from the CACP this month - one for his honors technical paper and one for his honors computer program submitted for certification. It is rare that a paper or program passes with honors, and this is the first time that an aspirant has received the award for both!

[redacted] Z211, became certified in Cryptanalysis this month.

[redacted] CACP Chairman, recently presided over a ceremony which announced the awarding of Technical Track titles to approximately 30 individuals. [redacted] (Ch. Z2), standing in for Tom Lessard, awarded the certificates.

(b)(3)-P.L. 86-36

(U) Congratulations to all on these accomplishments!

==========

f. ~~(FOUO)~~ CRYPTANALYSIS TECHNICAL TRACK UPDATE

~~(FOUO)~~ The CA Technical Track Review Panel (TTRP) is now accepting e-mail applications. Applicants should e-mail their persum and completed form P6770 to [redacted] and submit one signed hard copy version of each to the CA Career Panel office (H111, OPS 2B room 3036D). Contact the career panel office on [redacted] for more information.

****
//////////

5. (U) TECHNICAL CORNER

a. ~~(C)~~ Report On CRYPTO '95 (Submitted by [redacted] Z2)

~~(FOUO)~~ (The complete report will be distributed throughout Z, and can be obtained by e-mail to [redacted] Bob has offered to make copies of papers from the conference available also; again e-mail requests are easiest.)

(b)(3)-P.L. 86-36

~~(FOUO)~~ All of us know how popular CA-305 has become here at the Agency. You get to hear a selection of talks on contemporary developments in cryptology by smart people who have been working hard on a particular problem for perhaps a year and are ready to share their considerable knowledge with an audience. Instead of hard-working techies with a job to do, constrained by NSA perspectives and blinded by NSA objectives (as we all are), let the presenters be from around the world, researchers at major universities, probably all with doctorates, experienced lecturers, only minimally constrained by a modest teaching load, able to ponder the great issues of our day. Finally, place this enhanced (that is, if you prefer their subjects to ours) CA-305 in Santa Barbara, California (do you think you'd be in line for a Suggestion Award with this one?), in August, and you can see why the CRYPTO conference, sponsored by the International Association for Cryptologic Research (IACR), has become such a popular vacation for

[redacted]

(b)(3)-P.L. 86-36

so many people (of course the NSA representatives were hard at work, keeping the world safe for democracy, etc., so were never all on the beach at the same time).

(U) This was the 15th annual CRYPTO, and continued the uninterrupted string of successes. The attendance list which was circulated contained 330 names. Of those, 164 (almost exactly one-half) gave U. S. addresses. Among other countries, an astounding three-way tie resulted, with Canada, France, and Germany each having 21 attendees. Other nations represented were: Netherlands, 12; Japan, 11; Korea, 10; Israel, 9; Norway, Switzerland, each 7; Brazil, Denmark, each 5; Australia, Turkey, each 4; Belgium, Czech Republic, Hungary, Romania, Sweden, U. K., each 3; Austria, China, Singapore, South Africa, Spain, each 2; and Taiwan, 1.

(U) CRYPTO is a worthwhile meeting for NSAers to attend because it provides a window into the "academic" cryptologic community. Their "cryptology" is quite different from ours, reflecting the difference in their background, their goals, and their methods. They write books and papers which seem to be completely unrelated to what we think of as cryptology. Many of them would be unhappy (and very unsuccessful) as NSA employees.

(U) There were no seminal papers presented this year. Few people are capable of really first-class work, and academicians are limited (as we are not) by their quest for individual recognition. In a mature field like cryptology, where all the easy work has already been done, results are more readily obtained by sustained collaborative effort.

(U) The program was divided into 14 "sessions", two of which incorporated a single invited talk of some 45-50 minutes. The other 12 session topics included: number theory (2 sessions), cryptanalysis (2 sessions), secret sharing (2 sessions), MAC and hash, key escrow, protocols, "everything else", oblivious transfer, and zero-knowledge. (b) (6)

(U) There were two invited addresses, one by Adi Shamir, the other by [redacted] was billed as "NSA, retired", though very little of his career was spent as an Agency employee and, to my knowledge, he did not actively enter the cryptomath career field. He told a few of the usual war stories as though he had been there, but more likely he got them from David Kahn.

(S) Shamir's talk was better, but not by a lot. He too reminisced (maybe that's what was expected) about the events which led to the discovery (outside) of the RSA algorithm [redacted] He mentioned some difficulties that he and some of his colleagues had with NSA, but he tried to say that we were not too bad (after telling stories and showing viewgraphs that presented us in rather poor positions). Then he laid down the "Ten Commandments of Commercial Security". He gave as an example some recently cited figures on the per-year losses suffered by American banks. While check fraud costs $10 billion, credit-card fraud $700 million, and ATM fraud $18 million, losses to on-line fraud total only $5 million, so one should not go overboard designing security to defeat on-line fraud. He estimated that one needed to double the expenditure to halve the misuse, and such a heavy penalty was seldom justified, since most attacks are quite elementary. He cited an unnamed ex-NSA employee connected with the recent Venona release saying that he had enjoyed six or seven good days in 30 years of labor. Shamir compared his own

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

[redacted]

academic experience, which was just the opposite.

(U) We turn next to the unappealing rump session. Speakers were limited to five minutes, so nothing of any consequence was achieved. Anatoly N. Lebedev (LAN Crypto, San Jose) spoke on "New Regulations on Cryptography in Russia". There was something about the government seizing all the copies of some (international, with one of the Scandinavian countries?) conference report and classifying them.

(U) Bruce Schneier (Counterpane Systems) spoke on "Open Source SKIPJACK". The academic cryptologists are extremely curious about any classified cryptographic design, of course, and since SKIPJACK is under their noses they will pursue any avenue to ferret out information. I know nothing about it myself so, without guilty knowledge, I can report on the rumors which Schneier has collected (apparently a "Freedom of Information Act" suit against NIST has resulted in the release of some incompletely cancelled documents). There are 64 clock cycles per block: 2 clock cycles per round, 32 rounds; half of the text is not encrypted in each round; there is a 48-bit internal structure (versus 32 bits in DES); there is only half of the S-box data of DES; an unbalanced (the source blocks and the target blocks are of different sizes) Feistel network is employed; there are 2 clocks per G-box operation; 32 shifts per ECB function; the "F-table" of "SKIPJACK 3" was revised in 1992.

(U) John Gilmore (Electronic Frontier Foundation) keeps us posted on the progress of the anti-government knights, and at the moment the battle is to overthrow export controls on cryptography. He seemed pleased that the judge selected to hear the Dan Bernstein suit was formerly on the Board of the ACLU.

(U) David Naccache (Gemplus, France; coauthors, Markus Michels and Holger Petersen, both of the University of Chemnitz, Germany) distributed a useful technical paper "GOST 34.10 -- a brief overview of Russia's DSA". I quote from his paper:

"GOST 34.10 is Russia's DSA. Just as its U. S. counterpart, GOST is an ElGamal-like signature scheme used in Schnorr mode. It is close to NIST DSA in many aspects. In our paper, we will first overview GOST 34.10 and discuss the three main differences between the two algorithms."

"GOST's principal design criterion doesn't seem to be computational efficiency. This algorithm is 1.6 times slower than the DSA and produces 512-bit signatures. This is mainly due to the usage of the modulus q, which is at least 255 bits long. During verification, modular inverses are computed by exponentiation (while the extended Euclidean algorithm is roughly 100 times faster for this parameter size) and the generation of the public parameters is much more complicated than in the DSA. The choice of the parameters makes GOST 34.10 very secure."

"An advantage of GOST 34.10 over DSA is its inherent suitability to extended signature concepts, e.g., for blind signatures or multisignatures, as already shown in [two papers by Horster, Michels, and Petersen]. This property does not hold for the DSA."

(U) No doubt all of you readers gave already digested the paper "Why You Cannot Even Hope to use Groebner Bases in Public-key Cryptography: An Open Letter to Those Who Have Not Yet Failed" which appeared in the

(b)(3)-P.L. 86-36

9/23/2010

Journal of Symbolic Computation 18 (1994), 497-501. Its authors are Boo Barkee, Deh Cac Can, Julia Ecks, Theo Moriarty, and R. F. Ree. A footnote remarks that the last author was partially supported by SPECTRE. The authors are identified with Cornell University. Read backwards the name of the second author. The first is easily recognizable as "Bourbaki", the last as "referee"; who are the others?

(U) Jim Gillogly (RAND) described a successful attack on a 384-bit PGP (Pretty Good Privacy) key, solved by factoring the integer (it's the product of two primes, as usual) by harnessing 50 workstations, and using three weeks of MASPAR processing to complete half of the work. I think he said "modified", so maybe this wasn't a standard PGP key. To no one's surprise, he concluded that 384 bits is too short for a modulus.

(U) Cryptanalysts sometimes wonder how to acquire the mathematical knowledge we need (in a cryptologic situation where mathematics clearly applies) without getting enmeshed in a web of unnecessary theorems and proofs. In the case of elliptic curves, where a great deal of excellent but inapplicable mathematics is available, there is an answer, a good (by my standards) book by Alfred Menezes, "Elliptic Curve Public-key Cryptosystems".

(U) "How to Break Shamir's Asymmetric Basis", Thorsten Theobald (University of Trier, Germany). This was a very impressive piece of work, done while at the University of Frankfurt by a young researcher whom we have not seen before. I guess he must have been a doctoral student of Schnorr. He addresses a proposal of Shamir (CRYPTO'93), "Efficient signature schemes based on birational permutations". Shamir recommended two variants, a "symmetric" scheme and an "asymmetric" scheme. The first was attacked by Don Coppersmith, Jacques Stern, and Serge Vaudenay, but the attack depended heavily on the symmetry of the scheme. They showed how to forge a signature (that's what it means to "break" a signature scheme), but the secret key was not divulged. Theobald's attack transforms algebraic conditions into polynomial equations, then solves them, and finally recovers the key, thus completely breaking the scheme! The attack has been implemented, using Mathematica, on an HP 737/50 workstation, using 50-bit keys (the recommended key length is 512 bits; Theobald estimates a few hours for the attack in that case).

(U) "On the Security of the Gollmann Cascades", Sang-Joon Park, Sang-Jin Lee, and *Seung-Cheol Goh, Electronics and Telecommunications Research Institute, Korea. The German Dieter Gollmann has proposed "clock-controlled" cascades, and they have been much studied by the Chinese, but also by Menicocci and by Chambers. The Koreans specialize Gollmann's proposal to the case that each of the k registers (assumed to generate m-sequences, and with a senior register controlling the motion of its next junior) is of the same length n. Gollmann's proposal was not so restrictive. Another obvious weakness which you'd like to legislate away (but the Koreans have not, to their advantage) is the possibility of 0-stepping the registers. Both of these conditions (particularly the latter) contribute to the ease of solution which the Koreans report. Experimental results are given. They use, for the largest data set, n=100, k=9; they require 30 million consecutive bits of output and report using 55 minutes CPU on a Power Xplorer (Axil Hyundai) workstation (comparable, they say, to a SUN Sparc-10). For a more reasonable assumption, showing more respect for the cryptography, try "Analysis of Clock-controlled Sequences" by Xian Liu and Guozhen Xiao, from a recent issue of Applied Algebra in

(b)(3)-P.L. 86-36
9/23/2010

Engineering, Communication and Computing.

(U) "Improving the Search Algorithm for the Best Linear Expression", Kazuo Ohta, *Shiho Moriai, and Kazumaro Aoki (NTT). This was an excellent talk by a young Japanese woman. It is Matsui's deft development of the tools of "linear cryptanalysis" which has excited everyone, and those (few) who recognize the value of his work are able to present pretty good talks. The Japanese waste no opportunity to suggest the superiority of FEAL to DES; FEAL has no other champion. Their paper will appear (in English) in the first 1996 issue of the IEICE Transactions, section A.

(U) "On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm", Burton S. Kaliski, Jr. and *Yiqun Lisa Yin (RSA). Since Kaliski and Yin work for RSA, you'd expect their study of RC5 (designed by Ron Rivest) to give it high marks. They have tested it with straightforward differential cryptanalytic and linear cryptanalytic attacks and have, they claim (they offer no supporting computer experiments), determined that, for RC5 with a 64-bit block size (no alternative is considered), 12 rounds suffice to make both attacks impractical. Other researchers, viewing the same data, might have put a different spin: "9-round RC5 vulnerable to differential cryptanalytic attack!" Surely it's an accident that 12 rounds happens to be the exact specification laid down by Rivest! They conjecture (!) that the characteristics (for differential cryptanalysis) they have used are indeed optimal, and that the linear approximation upon which they have based their attack is also best.

(U) Key escrow is a hot topic with the CRYPTO crowd. "Escrow Encryption Systems Visited: Attacks, Analysis, and Designs", Yair Frankel (Sandia) and *Moti Yung (IBM). This seems to be rather an extensive analysis of potential weaknesses in both the "Clipper" and the "fair cryptosystems" approaches. The software key escrow methods of Trusted Information Systems (with which I am not familiar) also come within range of the Frankel-Yung scimitar.

CLAIM 1: There is an attack showing that the LEAF field in Clipper does not determine the identity of the chip which encrypted a message. Moreover, criminals can squeeze an honest person's LEAF in order to force escrow agents to open the honest person's escrow key. Claim 1 also tells us, they say, that users who have no part in some illegal action (whether knowing it or not) may have their keys opened and messages read.

CLAIM 2: There is an attack showing that compliance is not possible in Clipper given two rogue parties (even if the LEAF contains the identity of the parties' chips and proper integrity check).

CLAIM 3: Fair cryptosystems are not fair.

CLAIM 4: Spoofing is easy with public-key-based key escrow and the Clipper.

CLAIM 5: The Clipper puts compliance over availability.

CLAIM 6: Cheap Clipper chips may reduce the feasibility of the Clipper program for real-time Law Enforcement.

(U) "Robustness Principles for Public Key Protocols", *Ross Anderson and Roger Needham (Cambridge University, England). Anderson is an intelligent and practical cryppie. His advice is well supported. We excerpt from his paper.

PRINCIPLE 1: Sign before encrypting. If a signature is affixed to encrypted data, then one cannot assume that the signer has any knowledge of the data. A third party certainly cannot assume that the signature is authentic, so nonrepudiation is lost.

(b)(3)-P.L. 86-36

PRINCIPLE 2: Be careful how entities are distinguished. If possible, avoid using the same key for two different purposes (such as signing and decryption) and be sure to distinguish different runs of the same protocol from each other.

PRINCIPLE 3: Be careful when signing or decrypting data that you never let yourself be used as an oracle by your opponent. He illustrates with an example, published by Simmons, of an easy attack on a protocol of Tatebayashi, Matsuzaki, and Newman; this principle describes a very subtle and troubling difficulty which is not easy to defend against.

PRINCIPLE 4: Account for all the bits --- how many provide equivocation, redundancy, computational complexity, and so on. Make sure that the redundancy you need is based on mechanisms which are robust in the application context, and that any extra bits cannot be used against you in some way. Ignoring this principle created a weakness in ISO 11166, used by the SWIFT banking consortium.

PRINCIPLE 5: Do not assume the secrecy of anybody else's "secrets" (except possibly those of a certification authority). This one is supported by an attack of Mike Burmester on a RIPE protocol.

PRINCIPLE 6: Do not assume that a message you receive has a particular form unless you can check this.

PRINCIPLE 7: Be explicit about the security parameters of crypto primitives. A key generation routine should be claimed as good for so many keys; a threshold scheme for resistance to so many conspirators; a block cipher for so many blocks; and so on.

PRINCIPLE 8: Robust security is about explicitness; one must be explicit about any properties which can be used to attack a public-key primitive, such as multiplicative homomorphism, as well as the usual security properties such as naming, typing, freshness, the starting assumptions, and what one is trying to achieve.

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

(U) "A Key-schedule Weakness in SAFER-64", Lars R. Knudsen, Ecole Normale Superieure, Paris. Because SAFER was designed by the respected Jim Massey (ETH, Zurich, but he's an American) it has received much more attention than your average proposal. Knudsen's paper is significant because it represents a departure from standard attacks -- the key schedule has historically received little attention, maybe because in DES it was so carefully designed to be strong. As Knudsen admits, the resulting attack is not a serious threat to the security of the design; it merely shows that there is room for improvement. SAFER's recommended parameters include only 6 rounds of encryption. Knudsen's attack emperils this and also the 8-round model, but is sufficiently diluted by 10 rounds to be impotent. It applies equally to SAFER-128, but there Massey has already recommended at least 10 rounds.

(U) Research into factoring continues apace. I would like to quote from a marvelous article, by the marvelous Andrew Odlyzko (Bell Labs), which appeared in the RSA newsletter CryptoBytes. He starts by citing some historical milestones (at 10-year intervals) in factoring. In 1964 the record factorization was a number of 20 decimal digits. By 1974, a 45-digit number had been factored, using (as we now describe it) .001 mips-years (a mips-year is a year of processing on a VAX 11/780). By 1984, the corresponding numbers were 71 digits and .1

(b)(3)-P.L. 86-36

[redacted]

mips-years; in 1994, 129 digits (the RSA challenge) in 5000 mips-years. The recent RSA conquest has opened our eyes to the possibility of distributing the effort. If the Internet capacity is 3x10E7 mips (about 10% of the world's capacity) then the RSA challenge cipher drew 0.03% of Internet resources without much effort. Now that such a procedure has been shown to be effective, there is a reasonable prospect of acquiring much greater support for an attractive future effort. One could even consider the possibility of a clandestine attack. Odlyzko estimates that Silicon Graphics (well, you wouldn't have expected him to take Bell Labs as an example, would you?) has about 10,000 workstations (a total computing power of perhaps 10E5 mips, about 10 times that needed for the RSA129 project), so they are currently able (if they chose to do so) to factor a 512-bit integer in under a year of elapsed time. He mentioned that the success against the 384-bit PGP key (described by Gillogly in the rump session) used about 400 mips-years. Here's Odlyzko: "In a few years, we might see teenage system administrators for local real estate agents or laundries breaking 512-bit RSA keys without anyone being aware of the attack."

(U) A recent success by Dodson and A. Lenstra in factoring a 119-digit integer suggests to Odlyzko that the number field sieve (NFS) could have conquered RSA129 with only 1000 mips-years instead of the 5000 used by the quadratic sieve. He is able and willing to extrapolate from the extremely limited data (but he is a very smart guy, and experienced in these matters) a table of mips-years likely to be required to factor integers using the currently available NFS routines:

bits of n	mips-years
512	3 x 10E4
768	2 x 10E8
1024	3 x 10E11
1280	10E14
1536	3 x 10E16
2048	3 x 10E20

He estimated that moduli of 1280 bits should be safe for 20 years, and that even 1024-bit moduli should be safe unless they conceal extremely valuable information. But algorithms improve, and new techniques evolve. He is of course aware of the dangers posed by quantum computers and DNA computers, and that tools such as the "special NFS" apply in certain cases. In an appendix (there are ten of them!), Odlyzko compared DES to RSA, estimating that finding a single DES key would take about 300 times as much computing as the factorization of RSA129 (also, DES does not seem to be as vulnerable to a distributed attack).

****

b. (TSC) WORKING AND LIVING IN OTTAWA, CANADA
(Submitted by [redacted])

(TSCO) Canada's NSA equivalent, the Communications Security Establishment, (CSE), is located in Ottawa, the capital city of Canada, in the province of Ontario, about 550 miles from NSA and about 60 miles north of Ogdensburg, NY.

(TSCO) Working at CSE presents both similarities and differences from working at NSA. The first obvious difference at CSE (and also in Ottawa) is that most people are bilingual and many things such as signs, menus, etc. are written both in English and in French. Although English is the main language, it is not uncommon for coworkers to converse in French. Meetings and conversations with non-French

(b)(3)-P.L. 86-36

[redacted]

speaking people are always in English; therefore there is not a language problem.

(FOUO) Another difference at work is that it is more of a "laid back" atmosphere as compared to the hustle-bustle of the Agency. Many people wear shorts during the Summer and do some sort of recreation during lunchtime, this includes running, cycling, going for a walk, soccer, aerobics, working out at the nearby fitness center, etc. Cycling in Ottawa is especially popular with many people cycling to work.

(C-CCO) [redacted] There are informal afternoon "teas" twice a week in [redacted] (where I work) where someone brings in some food (e.g., cookies) and a "fun" problem, usually mathematical in nature, is lightly discussed.

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(FOUO) Living in the Ottawa area is a wonderful experience. [redacted]

(FOUO) Although warm by Ottawa standards, the summer was very pleasant and a nice break from the intense heat and humidity of Maryland. Canadians are said to thrive in the winter. Among other things, five miles of the Rideau Canal, which runs through the city, is open in the winter for ice skating. We are looking forward (with some trepidation) to the winter.

(b)(6)

(FOUO) Ottawa is a family oriented town with many museums and activities for families. There is an experimental farm in the heart of the city with exhibitions for families. Parliament Hill, where the federal government is, is also a popular attraction. For the sports fan, hockey has the Ottawa Senators of the NHL, football has the Ottawa Rough Riders of the CFL, and baseball has the Ottawa Lynx of the International League.

(FOUO) The cost of living is comparable to the Maryland area, maybe slightly higher but the value of the dollar more than makes up for the higher costs. (Currently, $1.00 US = $1.33 Canadian.)

[redacted]

(b)(3)-P.L. 86-36

[redacted]

****
//////////

6. COMMUNITY SERVICE

a. ~~(TSC)~~ CONSCRYPT NEWS

[redacted] CONSCRYPT-95 will be held from 30 October thru 3 November. The opening session will be held in FANX-2's auditorium. All other sessions will be held in A1B017 (Course Center B, FANX-2). There is limited seating at the Course Center B presentations.

****

b. ~~(FOUO)~~ IAI Trivia Contest Winners Announced

Rank	Score	Name	Org	Cash Prize
1	98	[redacted]		$250.00
2	91			$100.00
3	90			$50.00
4	89			Honorable Mention

(b)(3)-P.L. 86-36

****

c. ~~(FOUO)~~ S&E Presentation on FBI Use of Technology in Law Enforcement

(U) Law enforcement has various techniques which exploit scientific and technical principles. This discussion will relate how these techniques are applied to assist the investigator to develop indicators of criminal activity, determine the veracity of subjective evidence and establish the true fact of an investigation.

(~~FOUO~~) Since 1989 Special Agent [redacted] has served as the [redacted] for Technical Services in the Defense Criminal Investigative Service. He has a BS in Forensic Chemistry from [redacted] and a MS in Technical Management from [redacted]. During his four years in the Navy he served as a special agent in the Naval Investigative Service, conducting criminal, fraud and counterintelligence investigations. He then joined the Naval Investigative Service as a civilian.

(b) (6)
(b) (7) (C)
OGA

FBI

(~~FOUO~~) Special Agent [redacted] has served on several national level committees such as the DOD Forensic Service Advisory Committee and has been awarded the Meritorious Civilian Service Award.

****

d. ~~(FOUO)~~ MORE APPLES

(b)(3)-P.L. 86-36

(~~FOUO~~) [redacted] is collecting Giant, Safeway, and Metro Apples-for-the Students receipts again this year. All receipts will be donated to the Ruth Parker Eason School in Anne Arundel County. This is a special school for mentally and/or physically challenged children between the ages of 3 and 21 years old. These register receipts allow the school to purchase new computers, printers, software, and other educational tools for these special children. [redacted]

(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

7. (U) PUZZLES AND PROBLEMS

[redacted]

(U) EDITORIAL CORNER

NOTE: We MUST receive submissions for the November issue by 27 October

PLEASE NOTE: All submissions must be in ascii format, and, with the imminent implementation of E.O. 12958, MUST BE PORTION MARKED.

If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

(b)(3)-P.L. 86-36

[redacted]

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

(b)(3)-P.L. 86-36

TOP SECRET//COMINT

(C) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:18
(U)PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
November 1995

//

(TSUO) TABLE OF CONTENTS:

1. CA Perspective
2. Calendar of Events
3. KRYPTOS News
4. Word from the CACP
5. Technical Corner
6. Community Service
7. Historical Perspective
8. Problems and Puzzles

//

1. (TSUO) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of [redacted] D/Chief, J1.

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(S) Close your eyes for a minute and picture the future. Visualize the new game in town for cryptanalysts. Call up all we've been told about future processing, and I'm sure your inner screen will display something like this: [redacted]

[redacted]

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted] (b)(3)-P.L. 86-36

[redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) In trying to bring it to pass, J1 finds that many of the modules needed do not yet exist commercially. We must invent them, then get industry to sell them to us. But, there is a problem ... No one group of software or hardware experts at NSA has sufficient knowledge, expertise or manpower to construct the prototype. To succeed, the individual groups now groping with various aspects of the overall infrastructure must come closer together. We must evolve to resemble that which we would create: a cooperative, coordinated, scalable and philosophically unified network. And we will succeed ...

~~(S)~~ What does all this mean to the cryptanalyst? It could generate a whole new way of working. First, the analyst will become more engaged in

[redacted]

~~(S-CCO)~~ Certainly, the ability to manipulate data in a highly distributed network environment will become even more of a critical skill than it is now. The crypt community may, like the implementors of the infrastructure services, come to resemble a network: cooperative, coordinated, scalable and philosophically unified. After all, the future target is a network. Intelligence organizations tend to resemble their targets.

"""""""

by [redacted] (1000, R&E) (See 6a) (b)(6)

November 8 — IAI Presentation - [redacted] on "U.S. African Policy in a Time of Diminishing Resources" (OPS2B, 4118-6, 1200-1300)

November 17 — KRYPTOS Talk (TBA) and General Election (Friedman, 1300)

3. (U) KRYPTOS NEWS

a. Winners Announced at KRYPTOS Annual Banquet

(FOUO) Well over 100 people, including guests from GCHQ, a number of Distinguished Members, former Agency Employees, and current members and other Agency employees, attended the Annual KRYPTOS Banquet at the Fort Meade Officers' Club on the 26th of October. Nicholas Howard, Chief of H Division, and retiring after almost 40 years "in the business" spoke briefly about the highlights of the past, and provided encouraging words for the future. [redacted] out-going KRYPTOS President, and [redacted] President-Elect for 1996, emcee'd the proceedings, and everyone agreed that it was once of the best luncheons ever. [redacted] and her committee, [redacted] are to be congratulated for a job well done.

(FOUO) As is customary, the winners of the Annual KRYPTOS Awards were announced at this luncheon, and they were:

Distinguished Members 1995
[redacted] (b)(3)-P.L. 86-36

Peter Jenks Award
[redacted]

Norman Roberts Award
[redacted]

CA Literature Competition
1st Place - [redacted]
2nd Place - [redacted]
3rd Place - [redacted]
Honorable Mention - [redacted]

b. The election of KRYPTOS officers will be held in conjunction with the November presentation this month, on Friday November 17th.

(b)(3)-P.L. 86-36
[redacted]

4. (U) CACP NEWS

a. (U) MYSTERY ANALYSTS REVEALED

(FOUO) Even with clues posted mid-month, not many guesses were received to the identity of the mystery analysts for October. Correct guesses were received from [redacted]. The mystery analysts for October were...

A. [redacted]
B. [redacted]
C. [redacted] this was the one that stumped most people!)
D. [redacted]

(b)(3)-P.L. 86-36

(FOUO) Many thanks to those analysts who allowed us to feature them, and also to [redacted] who created the bulletin board display. Be sure to stop by the CA bulletin board in the 3rd floor breezeway between OPS 1 and HQS to check out November's mystery analysts. If you think you know who some or all of them are, reply to h111@nsa.

==========

b. (U) WELCOME FUTURE CRYPPIES

(FOUO) Two new CA interns joined our ranks this month:

[redacted] formerly a computer scientist in Z12
- formerly a computer scientist in J34

==========

c. (U) CHANGES

(FOUO) [redacted] has replaced [redacted] on the Computer Program Evaluation Board.

(b)(3)-P.L. 86-36

==========

d. (U) ANNOUNCEMENTS

(FOUO) The CACP is pleased to announce the following:

Promotion of CA intern [redacted] to GG-11.
[redacted], became certified in CA.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

==========

e. (U) CA Intern Profile

(S-CCO) [redacted] is currently in her third tour, working in [redacted] performing analysis on [redacted] Previous tours include [redacted] both of which she feels proved to be "quite illustrious".

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted] (b)(3)-P.L. 86-36 (b)(6)

(U) While considering the cryptanalysis career field, [redacted] was looking for career growth, which was very limited in her former career field. After interviewing with the panel executive, she was impressed with the mental challenge. When asked what she likes about the CA. intern program, [redacted] replied, "I find the coursework and exercises stimulating, and I look forward to reinforcing my newfound skills, while acquiring more with each diversity tour. Thus far, each tour has given me a new perspective of this obscure career field, its many dimensions, and its relativity to the Agency mission".

==========
//////////

(b)(3)-P.L. 86-36

5. (U) TECHNICAL CORNER

a. (FOUO) ENTHUSIASTIC REVIEW OF AN R51 DIVERSITY TOUR
(Submitted by [redacted])

(FOUO) On 9 January 1995, I walked into the R and E building, wound my way through several hallways, opened the door marked "R51 -- Math Research Division," and entered into a new world.

(FOUO) For 16 years I have worked hard at my job, but when I left the office, my classified projects stayed in my desk. During my six months in R51 I carried my project home with me every night and, on my day off, spent much of the day working on it. Since returning to Z43, my R51 project has continued to come to work with me almost every day, come home with me in the evening, and occupy much of my day off.

(FOUO) R51 -- a world of PhD mathematicians keeping up with math research all over the world. During the week of my arrival in R51, Dr. [redacted] from California spoke in the R5 auditorium on the topic of my project. During my last official week in R51 a recent PhD graduate, [redacted], spoke of work relating to the topic of my project which was the subject of his PhD dissertation. In between these two speakers were speakers and classes in all areas of mathematics, a weekly algebra seminar, a class on the new discovery of codes derived from elliptical curves, reports from attendees at math conventions, talks on research being conducted, etc. Two weeks of the algebra seminar were devoted to my project -- the [redacted] I briefed twice while in R51.

(b)(6)

(FOUO) For two months my office mate was a professor from Clemson University who comes to NSA for two months every summer as a consultant.

(FOUO) Perhaps I have now aroused sufficient curiosity as to what my R51 project was. In the past three years, [redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted] My task has been to understand the papers written on this new topic, and to write a paper to clearly describe the results and to make mathematically rigorous all the results that have been published. The writing of the paper has been very complicated because I have attempted to make it readable to those with little background in [redacted] Both topics are presented in the paper. (b)(3)-P.L. 86-36

(FOUO) One of the most fun and exciting experiences for me was doing research in the R51 library. Of about 50 references that I looked for, 45 were in journals already at the NSA library. Every article that I needed in an existing journal was in the library in the place it was supposed to be. The copy machine was available to copy found articles without charge. The articles not in the library were requested for me over interlibrary loan and were in my hands within several weeks -- even one written in German.

(FOUO) Even though R51 has many PhD mathematicians, there is a place there for all types of people. What is needed is a love of mathematics and a desire to learn more about mathematics. Many of the people in the office are teachers as well as research mathematicians and they are skilled at suggesting projects for anyone in their care and at working with that person to help in the completion of a project. I highly recommend a tour in R51 for anyone in the mood for mathematics, research, hard work, and fun.

(FOUO) I am glad to be back in Z43, but my life will never be the same. It is no longer true that there is nothing work-related that I can do when I go home in the evening. There is always new math research that can be explored. I plan to keep up with all math research relating to my R51 project, and I will be involved in looking for uses of [redacted] in the real world. I have yet to learn about the [redacted] in R51, which was one of my goals while I was there. I want to take some time to go back and learn about this topic. My time in R51 was not only rich and rewarding, but also life-changing. I hope to complete my paper soon, so that analysts at NSA can benefit from my research. (b)(1) (b)(3)-P.L. 86-36

b. (FOUO) A KRYPTOS Yankee in King Arthur's Court

(Submitted by [redacted])

(FOUO) Please think of the following as a friendly note from me to you. It documents significant aspects of our PCS (permanent change of station) experience at Menwith Hill Station, North Yorkshire, 1991-1996. Loosely and interchangeably, the "us / our" descriptors refer to myself, my husband, occasionally my 2 year old Yorkshireman son, new but lasting British and American friends, acquaintances, and various MHS associates. (b)(3)-P.L. 86-36

(U) To begin, I'll chat about the weather; ... most appropriate, since the weather is always the conversation starter. North Yorkshire's weather is unique ... we think it's "just brill" when the sun hangs before its backdrop of blue sky and sparkles as the puffy clouds whisk by; ... on the other hand, we wonder what is hitting us when the horizontal rain challenges our efforts to move from one location to another. Despite the weather's contrasts, we endure and enjoy other aspects of living.

(U) To name a few, ... we have fortunately exposed ourselves to a

respectable subset of the innumerous travel and cultural opportunities. Our passports and scrap books are impressive with various country stamps and tickets. England features strategically placed air and ferry ports which easily facilitate "going to the Continent", as the locals would say, or hopping over to Ireland. The rail system networks throughout the United Kingdom: London and Edinburgh are popular destinations that may be obtained in a matter of seemingly effortless hours from York, the North Yorkshire midpoint. Abbeys and ruins decorate the countryside, welcoming us to explore them and picnic on the grounds while taking a break during our Sunday drive. Cathedrals adorn the city ceners, drawing our attention above the streetview market places. British artisans display their wares in local shops and markets, and they usually enjoy passersby to observe them develop their creations. Many food and beverage items are prepared locally and still by hand, like the Wensleydale cheeses and Brymore ice creams as well as the John Smith bitters and the Black Sheep ales. Publicans, the curators of public houses, more commonly known as pubs, encourage the locals to have a pint, and maybe even a meal. It should also be noted that Brits, a socially acceptable slang term to describe British subjects, love their animals; ... so much so, we usually see dogs accompanying their masters rather than children their parents in the older traditional locals. Given the last sentence, it would be most appropriate to now comment on language. We have learned through experience that America and Britain are certainly two countries divided by a common language.

(U) Shopping is a topic which should next be addressed. Most shopping is completed by knowing what you set out to purchase and knowing from which shops to purchase them. Your local butcher provides your meats, and the fishmonger provides your seafood, and the green grocer provides your fresh produce, the weekly market in the town square hosts vendors for other household items, the hardware store supplies tools and equipment; ... I think you get the idea. Within the last decade, supermarkets, department stores, and malls have blossomed around the country and have really responded positively to customer demand.

(U) Medical care is a function of two caregiver systems. The National Health System (NHS) cradled us during the pregnancy, birth, and early months of life for our Yorkshireman son. Midwives, health visitors, and doctors provided great advice and care before, during, and after; and they even made routine house calls! For common NHS visits, service is rendered with no accompanying pricetag. On the other hand, when one "goes private", as we did when our son suffered from recurrent ear infections, we received bills for the service rendered. We then submitted these bills to our Blue Cross/Blue Shield Health insurance plan and were swiftly reimbursed the usual 80-85%. "Going private" simply means that an individual is soliciting care from a doctor who maintains his/her own private practice, perhaps in addition to the NHS clinical practice. Basically, funding makes resources available, so "going private" allows for patients to receive care in terms of more options. Incidentally, by being a Yorkshireman, our son is entitled to play for Yorkshire cricket, positions only traditionally held by Yorkshiremen.

(U) Housing is another topic for discussion. We have had the opportunity to live in three different homes: a direct result of availability and a landlord's change of status from employment to retirement. Not only do we now consider ourselves professional movers, but we have enjoyed living in various landscape settings, neighborhoods, and home structures: from the dales to the farm, from a bridal path lane to a village, and from the quaint cottage with all

modern amenities to the refurbished brownstone to the modern home.

(U) And, oh, yes, work, the foundation for a PCS, is now an aspect which warrants comment. Given the small but expanding infrastructure, work requires us to tap on the sources of our diversity. For example, duties and responsibilities defined by mission allow for flexibility as mission requires. Furthermore, many individuals play significant roles in various committees and meeting groups. The reasons for these two examples clearly stems from the small numbers and the transient nature of a field site.

(FOUO) We hope that this short synopsis provides you with some useful information and an inviting "warm fuzzy" about a PCS tour at Menwith Hill Station.

****
//////////

6. (U) COMMUNITY SERVICE

a. (U) Science and Engineering Society Presentation

(U) In this talk, [redacted] who is the Director of the Center for Satellite and Hybrid Communications Networks, will address the advancements in communications and network technologies and how this technology has created real opportunities for the creation of an information infrastructure that provides mass access digital connectivity at affordable costs. He will discuss various technical challenges imposed by the increased need for digital connectivity and the on-going programs of research in hybrid internetworking, wireless networking, digital libraries, databases, telemedicine and personal computing and communications systems. He will describe some unique opportunities for rapid advancement in digital connectivity, by means of some recent technology transfer results he has achieved.

(b) (6)

(FOUO) [redacted] received a B.S. in Electrical Engineering, with highest distinction from the National Technical University Athens, Greece in 1970 and a M.S. and Ph.D. in Applied Mathematics from Harvard in 1971 and 1973 respectively. Since 1973 [redacted] has been on the faculty in the Department of Electrical Engineering at the University of Maryland College Park as a professor of Applied Mathematics. From 1985 to 1991 he was the Founding Director of the Systems Research Center now the Institute for System Research. In February 1990 he was appointed to the Martin Marietta Chair in System Enginering. Since 1991 he has been the Director of the Center for Satellite and Hybrid Communications Networks, a NASA center for the commercial development of space, which he co-founded. [redacted] has held visiting research scholar positions with Stanford, MIT, Harvard and the University of California, Berkeley. He has numerous publications in control and communications systems, and is the co-editor of Recent Progress in Stochastic Calculus, Springer-Verlag, 1990. His current research interest includes stochastic systems, signal processing and understanding with emphasis on speech and image signals, real-time architectures, symbolic computation, intelligent control systems, robust nonlinear control, distributed parameter systems, hybrid communications network simulation and management.

THIS SYMPOSIUM WILL BE BROADCAST OVER NEWSMAGAZINE CHANNEL 17

ALL PERSONNEL ARE WELCOME

(b)(3)-P.L. 86-36

[redacted]

For information on or membership in the Science and Engineering Society contact Tom Kline [redacted] (b)(3)-P.L. 86-36

b. (U) International Affairs Institute (IAI) Presentation

(U) [redacted] the current Director of Regional Affairs in the Office of the Assistant Secretary of State for African Affairs, and former NIO for Africa, will address the topic of U.S. African Policy on Wednesday, the 8th of November, at noon. IAI members will be seated on a priority basis until 1145. (b)(6)

c. ~~(FOUO)~~ Communications Analysis Association (CAA) Presentation

~~(C-SCO)~~ The CAA is proud to announce its first Membership Meeting and the first of its sponsored presentations will be held on Monday, November 6th. [redacted] of the Joint Military Intelligence College will discuss "The Nature and Process of Analytic Thought". The program will include a welcome by CAA President [redacted] and a question and answer period with [redacted] The classification level of the talk will be TOP SECRET UMBRA, and all Green and Gold Badge personnel are welcome to attend.

d. (U) APPLES FOR THE STUDENTS

(U) CMI is pleased to support two schools this year in the Apples for the Students program, Ruth Parker Eason and the Imaculate Conception School. Giant, Safeway, and Metro receipts are being accepted.

(U) Ruth Parker Eason is a special school for mentally and/or physically handicapped children. Ages of the students attending the school range from 3 to 21 years old. The school is located in Anne Arundel County. The register receipts that were donated to them two years ago were equal to what they collected on their own. The purchased equipment was particularly useful to a school with their needs. Please receipts to be donated for this school to [redacted] [redacted] HQ. (b)(3)-P.L. 86-36

(U) Immaculate Conception school at 7 th and N street N.W., Washington, D. C. Immaculate Conception is in a very low income part of the city. It is a very needy school. Although it is a school supported by the parish(catholic) over 90% of the children are a different faith and not members of the parish. Receipts to be donated to this school should be sent to [redacted] R51.

//

7. (U) CRYPTOLOGIC HISTORY (b)(3)-P.L. 86-36

a. (U) ROTOR DEVELOPMENT HISTORY

~~(S)~~ One of the major milestones in the history of machine cryptography was the invention of the rotor as a basic component for the performance of the encrypting/decrypting operation in mechanical and electro-mechanical cipher equipment. Available evidence indicates that the wired rotor was originally conceived by H.A. Koch, a Dutch

[redacted]

inventor, during the years preceding World War I, and it found its first practical use in the German Enigma machine. Almost simultaneously, it was invented and patented in a somewhat different form by E. H. Hebern, an American. Another contribution to the art was made by Sidney Hole, a farmer from Devonshire, England, who conceived and patented a cipher machine which utilized pneumatic rotors.

~~(S)~~ The subsequent history of the development of electrical wired rotors in the U.S. is one of evolutionary progress through the succeeding years. In the later 1920s the U.S. Navy contracted with Hebern to build a wired rotor cipher machine for military use. The first results of this development were not completely successful and because of legal difficulties of a patent, no further work was performed by Hebern for the U.S. Government. In the years following World War II, equipment was finally evolved which became the major high echelon cipher equipment used by the U.S. during World War II. It was based upon the concept of a wired rotor maze and included the principle of enciphered motion developed by Mr. W. F. Friedman and Mr. Frank Rowlett. Under the direction of Captain L. F. Safford, USN, Teletype Corporation developed and produced this equipment known in the Navy as the CSP-889, or Electrical Cipher Machine (ECM), and in the Army as the SIGABA.

****
//////////

8. (U) PUZZLES AND PROBLEMS

(b)(3)-P.L. 86-36

a. ~~(FOUO)~~ Solvers and Solutions

~~(FOUO)~~ At least partial solutions to the September puzzle were received from [redacted] They got the correct ordering in the first part - number the letters from a=1 to z=26, and sum the values of the letters in each word. Arrange the words in order from smallest sum to largest. To answer the second part, the words can be arranged in order (below) so that the last three letters of one word and the first three letters of the next word also make a word. When you get them all right, you have a start word and an end word, an the three letters which connect them are TOR. Number the top row of the keyboard from Q=1 to O=9 to get TOR=594.

(U) portal entrap pelmet richer ballad ledger billet termed usable aching lessee kernel sonata mantra cervix ensign oregon adsorb italic TOR

****

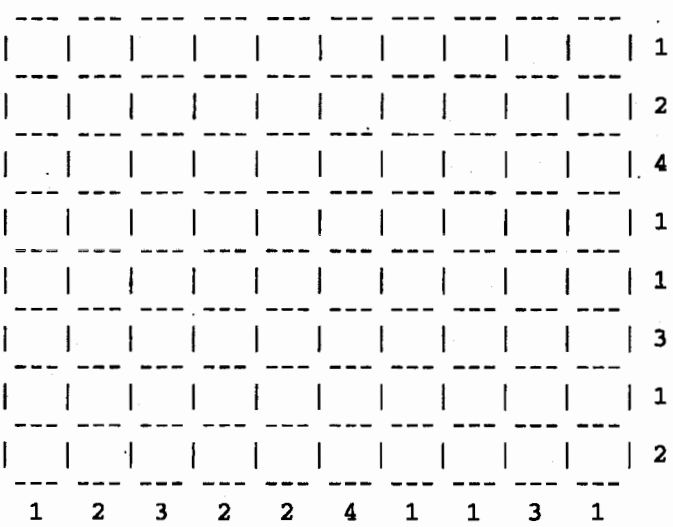
b. (U) This Month's Challenge

(U) In this solitaire version of the popular "Battleship" game, you are to find the 10 ships listed below. The ships will lie either vertically or horizontally (never diagonally) on the grid. The numbers on the side and bottom of the grid tell how many squares in that row or column, respectively, have ships in them. (For example, the "1" next to the top row means that one square in that row is taken up by a ship, but it's up to you to find where, and what kind of ship.)

									1
									4

(b)(3)-P.L. 86-36

[redacted]



1 Battleship: XXXX
2 Cruisers: XXX XXX
3 Destroyers: XX XX XX
4 Submarines: X X X X

(U) Submit solutions (and proposals for future puzzles) to [redacted]
([redacted]

(b)(3)-P.L. 86-36

(U) EDITORIAL CORNER

NOTE: We MUST receive submissions for the December issue by 27 November.

PLEASE NOTE: All submissions must be in ascii format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

(b)(3)-P.L. 86-36

[redacted]

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

(b)(3)-P.L. 86-36

TOP SECRET//COMINT

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:17
(U)PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
December 1995

//

********** NOTICE ********* NOTICE ********** NOTICE **********

(FOUO) OYEZ! OYEZ! OYEZ! CALLING ALL ALMOST-RETIREES! How about writing an article about the most memorable "happening(s)" during your career here? We will then feature these in upcoming newsletters. Please take the time to leave a little legacy to those of us who are still here! (Ascii format, please, and send to [redacted] (b)(3)-P.L. 86-36

*********ANOTHER NOTICE **********ANOTHER NOTICE **********

(U) Please note the short suspense for input to the next issue. We hope to distribute the issue by December 20th or so, before many of our readers depart for the Holidays.

****

(FOUO) TABLE OF CONTENTS:

1. (U) CA Perspective
2. (U) Calendar of Events
3. (FOUO) KRYPTOS News
4. (FOUO) Word from the CACP
5. (U) Community Service
6. (U) Literary Tidbits
7. (U) Problems and Puzzles

(b)(3)-P.L. 86-36

//

1. (FOUO) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice: This month we are pleased to feature the thoughts of [redacted] Chief, Z5.

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TSC)~~ The lesson, if obvious, is often hard to apply. It might be difficult for us to share our data and our early discoveries because we want to do the entire problem. This attitude, while understandable, is costly. Often, to solve our problems in the best manner, we must take the time and effort to share them. Our management has a responsibility to create and nurture such an environment. [redacted] and I meet weekly to try to foster this attitude between Z2 and Z5. The Z4-initiated [redacted] Exchange Group is an excellent example in which analysts share their problems.

(b)(3)-P.L. 86-36

~~(TSC)~~ Currently Z Group is attempting to define its role in [redacted] Tom Lessard, recognizing these problems, has charged his Office Chiefs with defining the Z Group management model for active network attacks. If we are to be successful, one ingredient is a big need for inter-office trust and cooperation. We will try to make that happen.

(U) Our future successes will depend on our working together closely in a large community. This will require high levels of trust and confidence. We need your help.

****
//////////

2. (~~TSC~~) CALENDAR

Dec 14	NSA Science and Engineering Society presentation, "The Threat to the Department of Defense Information Infrastructure", by [redacted] (R & E Symposium Center, 1000)

(b)(3)-P.L. 86-36

PLAN AHEAD for 1996

Jan 17	Second Annual Breakfast for Newly Certified Cryptanalysts (BANCC), (Canine Suite, 0800-1000)
Jan 19	Joint CMI-KRYPTOS Talk, "INFOSEC Posture and Threat", by Rick Proto, Chief R. (Friedman, 0900)
Mar 14	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)
Mar 25-29	CARD
May 13-17	ACE 1996 at CCS in Bowie.
June 18	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)

[redacted]

Sep 17	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)
Fall?	CONSCRYPT '96, at DSD
Nov 19	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)

//

3. (~~FOUO~~) KRYPTOS NEWS

a. (~~FOUO~~) On 17 November the Kryptos Society held its annual election, with the following results.

President-Elect	[redacted]
Treasurer	
Member-at-Large	
Member-at-Large	

(b)(3)-P.L. 86-36

(~~FOUO~~) Our thanks to those who agreed to run, and special thanks to those outgoing Council members who have served so well: [redacted] Treasurer, Floyd Weakley and [redacted] Members-at-Large. And, of course, a BIG THANK YOU to our outgoing President, [redacted]

b. (~~FOUO~~) Joint KRYPTOS-CMI Presentation

(~~S-CCO~~) Rick Proto's presentation characterizes the successes of the [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

c. (~~FOUO~~) Second Peter Jenks Community Service Award Presented

(~~FOUO~~) At the KRYPTOS Fall Luncheon in October, the winners were announced for the Literature Contest, the Peter Jenks Community Service Award, and the Norman Roberts Award. In the following months we will be highlighting some of the recipients of these awards. This month we will focus on the Peter Jenks Award winner, [redacted] citing the recommendation that came to the Council.

(~~FOUO~~) [redacted] recently completed an extended term as Chairman of the Cryptanalysis Career Panel. He was an eloquent spokesperson for the community, raising the morale of and professional esteem for cryptanalysts throughout NSA. His contributions include:

(b)(3)-P.L. 86-36

(~~FOUO~~) - Establishment of the annual Cryptanalysis Conference. His vision of an event that would bring cryptanalysts together to assess their posture and future was met with skepticism by the members of the Panel; only his advocacy made it a reality. Now in its third year, this event is providing an opportunity for cryptanalysts to address crucial issues while simultaneously fostering a sense of community. Bob has not hesitated to raise contentious issues at the conferences, enabling the community to recognize, discuss, and work to resolve

(b)(3)-P.L. 86-36

[redacted]

them.

~~(FOUO)~~ - Training. Following-up on his participation on the CA Curriculum Review Board, Bob personally participated in the development of two new cryptanalytic courses, CA-112: [redacted] and CA-219: Advanced Cryptanalytic Techniques. He participated in pilot offerings of both, providing guidance in the content, instruction and exercises presented to the students. In addition, he has worked one-on-one with countless junior analysts, personally nurturing their technical development.

~~(FOUO)~~ - Gold Bug Award Recognition. The Gold Bug Award is potentially one of our most powerful public relations tools. Shocked that our awardees were languishing in obscurity, he proposed a permanent plaque be installed for the award, and that the Director, himself, dedicate it. He suggested that the originators of the award participate and be recognized, along with all past recipients. The ceremony was held exactly as he had envisioned, and brought great honor to our career field. The plaque now hangs in OPS2B, along with others that recognize outstanding accomplishments of NSA employees.

(b) (3)-P.L. 86-36

~~(FOUO)~~ - Gold Bug Team Award. Under [redacted] leadership, the CACP established the Gold Bug Team Award to recognize teamed efforts against our increasingly difficult technical challenges. He planned and presided over the inaugural presentation of this award in 1994.

~~(FOUO)~~ - KRYPTOS-CACP Partnership. [redacted] recognized that together, KRYPTOS and the Cryptanalysis Career Panel might prove a more effective force to strengthen our community than either entity could alone. He approached the president of the KRYPTOS Society and arranged a joint session of the two groups. That historic meeting produced an extremely large number of excellent suggestions and directly resulted in the very successful community newsletter "Tales of the Krypt". The newsletter has established a new and effective means to disseminate information and feedback. This very award, The Peter Jenks Award, was conceived at that joint meeting as well.

~~(FOUO)~~ Though the Panel's participation in the Technical Track Program was hardly optional, through his leadership, the CA career field implementation of the Agency program has stood as a model to which other disciplines aspire. The CA Technical Track Review Panel was the first to begin assessing applicants and the first to honor participants with a titling ceremony. Bob has represented our concerns at many Senior Technical Track Board (STTB) meetings, helping to fashion a plan that could work for our field.

~~(FOUO)~~ - CACP Subcommittee participation. In addition to leading the CA Career Panel, Bob has, over the course of his tenure on the Panel, volunteered his technical expertise for each subcommittee assessing aspirants for certification. Bob has worked on the PQE committee almost since its inception, and has served terms on both the Paper and Program committees.

~~(FOUO)~~ - Aspirant Interviews. Bob personally undertook a series of interviews with aspirants for CA certification to assess the fairness of the process and to ascertain if and where changes were needed.

~~(FOUO)~~ The initiatives described above are only the most visible portion of [redacted] contributions to the Cryptanalysis career field. Throughout his tenure he invested much time, energy and emotion

(b) (3)-P.L. 86-36

[redacted]

pondering the issues that face the career field. His subtle, yet effective influence has moved the community in new directions. For those of us who have worked with him on these community endeavors, he has been a mentor and a hero. Again, we are proud to present him as a most deserving candidate for the Peter Jenks Community Service Award."

****
//////////

4. (~~TOUO~~) CACP NEWS

a. (U) Professionalizations

(~~TOUO~~) Two people completed their requirements for CA certification:

[redacted]

Congratulations to them both!

---

b. (~~TOUO~~) Changes to CACP

(~~TOUO~~) The CACP is pleased to announce two new panel members:

Computer Science Advisor - [redacted]
Math Advisor - [redacted]

(b) (3) -P.L. 86-36

---

c. (U) MYSTERY ANALYSTS REVEALED

(~~TOUO~~) Only two people submitted guesses for this month's mystery analysts. [redacted] correctly identified analysts B, C, and D. The CA Executive regrets that no clues were posted mid-month due to the fact that she was in class and then furloughed! Nevertheless, November's mystery analysts were as follows:

A. [redacted]
B.
C.
D.

(~~TOUO~~) As a side note, November's mystery analyst C used to play volleyball with October's mystery analyst A [redacted]!

(~~TOUO~~) Our thanks to those analysts who allowed us to feature them, and also to [redacted] who created the bulletin board display. This month's low rate of participation was somewhat disappointing, but we will try one more month of the Mystery Analyst contest to see if there is any interest in it continuing. We welcome your comments and/or guesses at the CA Career Panel office (h111@nsa). Be sure to stop by the CA bulletin board in the 3rd floor breezeway between OPS 1 and HQS to check out December's mystery analysts.

(b) (3) -P.L. 86-36

---

d. (~~TOUO~~) 1996 CA Conference Planning Underway

(~~TOUO~~) The CA Career Panel has begun considering topics for the annual

[redacted]

CA conference in March 96, and is soliciting suggestions from the CA work force. If you have an issue/topic/concern that is of widespread interest to cryptanalysts, please forward your suggestion (with a brief explanation) to the CACP office (h111@nsa) by 14 Dec.

****

//

5. (U) COMMUNITY SERVICE (b)(1) (b)(3)-P.L. 86-36

a. ~~(FOUO)~~ Winners of First Stephen W. Dilke Award Announced at CANUKUS Crypto-T/A Conference

(C) Delegates from CSE and NSA, including [redacted] joined GCHQ analysts for the 1995 CANUKUS Crypto-T/A Conference from 17 through 19 October. This year's conference was opened with the announcement of the first winners of the Stephen W. Dilke Award for using Crypto-T/A to make a significant contribution to intelligence - the theme of this year's conference.

[redacted] (b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

Along with discussions stressing a CANUKUS agreed statement on improving the Value for Money provided by Crypto-T/A, the 1995 Crypto-T/A Conference featured nineteen speakers presenting highlights of Crypto-T/A's contributions to intelligence on twenty-two different topics, well achieving this year's theme.

****

b. ~~(FOUO)~~ Science and Engineering Presentation

~~(FOUO)~~ [redacted] of the Defense Information Systems Agency, will speak at 1000 hours on Thursday, December 14th in the Research and Engineering Symposium Center. The Title of [redacted] talk will be: (b)(6) OGA DISA

"The Threat to the Department of Defense Information Infrastructure"

~~(FOUO)~~ [redacted], whose organization is responsible for assessing and pententrating DOD networks, will address their astonishing successes to

(b)(3)-P.L. 86-36

[redacted]

date. [redacted] will also discuss the implications of risk managment vs. risk avoidance and DISA's Defensive Information Warfare program.

(b) (6) OGA

(TOUO) [redacted] has ten years of experience as a counterintelligence officer in the US Army and fifteen years of experience as a DOD civil servant in the field of secure communications networks. [redacted] is a graduate of the State University of New York and has over 500 class room hours of technical post-graduate work in information systems. [redacted] has received several military and civilian awards for [redacted] outstanding work in the secure communications area.

DISA

****
//////////

6. (U) LITERARY TIDBITS

(U) {EDITORS' NOTE} Given our recent FURLOUGH experiences, thought the following, which appeared on ENLIGHTEN, from an unidentified author, rather appropriate.
+++++

"Sometime when you're feeling important.
Sometime when your ego is in bloom.
Sometime when you take it for granted
You're the best qualified in the room.
Sometime when you feel that your going
Would leave an unfillable hole.
Just follow this simple instruction
And see how it humbles your soul.

Take a bucket and fill it with water.
Put your hand in it up to the wrist.
Pull it out and the hole that's remaining
Is a measure of how you'll be missed.

You may splash all you please when you enter.
You may stir the water galore.
But stop and you'll find in a minute.
That it looks quite the same as before.

The moral in this quaint example
Is do just the best that you can.
Be proud of yourself but remember
There's NO indispensable woman or man."

****
//////////

7. (U) PROBLEMS AND PUZZLES

a. (TOUO) We received solutions to last month's puzzle from [redacted]

One solution to the puzzle is:

OOOOOOOXOO
XXXXOOOOOO
OOOOXOOOOO
OOOOOXOOXO
OXXOOXOOXO

(b)(3)-P.L. 86-36

[redacted]

OOOOOXOOOO
OOOOOOOOXO
OOXXXOOOOO
OOOOOOOOOX
OOOOOXXOOO

Many others are possible.

****

b. (U) December's Puzzle

~~(TSSC)~~ Here's a puzzle [redacted], our Puzzle Editor, got from [redacted] would like to remind everyone that he would love to have others submit puzzles to him for future issues!

(U) For this puzzle, the words are already ordered. The list was originally 40 long, but the escape from the Nile of a rat has reduced it to 38 (read down the columns). Identify the 8 themes within the list, and recreate the original.

is	hear	cure	through
pair	party	compromise	sitting
prepared	hum	broad	punch
sin	print	henry	talk
cat	derby	dear	buds
out	fruit	money	williams
brown	legal	shoes	thieving
clock	bridge	red	base
culture	purchase	hood	pudding

(b)(3)-P.L. 86-36

****
//

##

(U) EDITORIAL CORNER

REMINDER: Submissions for the January issue are due by December 15th.

PLEASE NOTE: All submissions must be in ascii format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(TSSC)~~ EDITORIAL BOARD

[redacted]

[redacted]

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

Return to Kryptos Home Page

NSA Home Page

(b)(3)-P.L. 86-36

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

[redacted]

~~TOP SECRET//COMINT~~

(S) POC: [redacted] info
(U) *Last Modified: 10/30/2002 11:42:20*
(U) PE EXTERNAL PAGE

THE CLASSIFICATION OF THIS NEWSLETTER IS ~~TOP SECRET UMBRA~~

****
* TALES OF THE KRYPT *
****

(b)(3)-P.L. 86-36

January 1996

HAPPY NEW YEAR TO EVERYONE!

//
****

~~(FOUO)~~ TABLE OF CONTENTS:

1. (U) CA Perspective

2. (U) Calendar of Events

3. ~~(FOUO)~~ KRYPTOS News

4. ~~(FOUO)~~ Word from the CACP

5. (U) Community Service

6. (U) Literary Tidbits

7. (U) Problems and Puzzles

8. ~~(FOUO)~~ Editorial Corner

//

1. ~~(FOUO)~~ PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of [redacted] SUSLOC.

(b)(3)-P.L. 86-36

~~(FOUO)~~ My first inclination was to write a straightforward article about the virtues of a tour for a cryptanalyst at the Defence Signals Directorate, Australia's national SIGINT authority, when [redacted] kindly asked recently if I would write an article for 'Tales of the KRYPT'. I decided, however, to take an entirely different slant though it's one that still focuses on the cryptanalytic career field. (By the way, I use the term 'cryptanalytic' in a broad sense. It would include, among others, everybody in Z Group. Further, I submit much of the thrust of what I will be saying has relevancy throughout NSA today.) I will reveal the driving force behind the change of mind later.

~~(FOUO)~~ Try to imagine a job that combines fun with high stakes, one where success can markedly improve your country's well-being. Try to imagine one whose importance goes off the top of the scale, where the challenges never go away, where success is often tantalizingly close -- and indeed often realized -- and the payoffs can be of incredible

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

value. Further, try to imagine a field where one can commit oneself to every aspect of the job from long-term research to hands-on practical applications during a career.

(FOUO) If those aren't enough attributes, consider one where an abundance of good data to work with is the rule rather than the exception, albeit in many cases not without a great deal of effort involved. Consider one where the tools provided are a cut -- actually, several -- above those found virtually anywhere else. Consider one where teamwork is invariably a necessary though not always sufficient condition for success and the caliber of those comprising the teams is arguably as high as that to be found anywhere. Consider one where you might be fortunate enough to participate in an international cooperative effort in intelligence the likes of which the world has never seen. (I'm talking, of course, about the UKUSA Agreement and what it has become over the last half century. It is my contention there has never been a more durable one in recorded history nor one where the bandwidth of the exchange was higher. Those skeptical should ask CIA.)

(FOUO) You have long since realized where this was leading. Most of you reading this fall into the category of those fortunate ones I'm talking about. You're working at a place, NSA, that has one of the most important missions charged to any component of the U.S. government. My experience has taught me there is no more gifted set of people anywhere in this world, and I'm speaking particularly of other U.S. intelligence agencies, foreign intelligence agencies and U.S. industry when I say it, based on firsthand observations. You're working in a field of endeavor that is frequently referred to as NSA's core discipline. There's nobody else like you anywhere in the government. The caliber of your peers is unsurpassed.

(FOUO) Let's talk about opportunities. On the technical level, while the challenges continue growing, I submit they are just that. They have been growing for years and they have largely been met. I note the amount of plain text produced has grown almost uninterruptedly for years. You set yet another record last year. I expect both the number of challenges and successes to continue.

(FOUO) On a personal career level, our Agency has become one over the past ten or fifteen years where we are fortunate in that an individual may follow either technical or management tracks. It wasn't always like this at NSA and, frankly, it isn't like it at most other places even today. The approach may have some flaws, but one only needs to have been around about half as long as I have to remember what it used to be like.

(FOUO) What does the future hold? Access will be harder. Volumes will be greater. Getting at the data of interest will become increasingly challenging. Stakes will continue increasing. Boundaries between disciplines will continue becoming fuzzier. Challenges? Certainly. Opportunities? Ditto.

(FOUO) Why am I using so many words simply to state the obvious? Frankly, I'm not so sure it's obvious. Let me explain where I'm coming from. I've been ten thousand miles away for thirty months. While I certainly have no feel for the mood of the place on a day-by-day basis, a couple of factors tend to compensate for it. First, as do most field chiefs, I come back for a week or two every six months. Second, e-mail, while no substitute for being there, does pretty well in keeping one abreast of how people feel. I get the sense a few people - or just maybe more than a few - have lost sight of what they have going for

(b)(3)-P.L. 86-36

them.

~~(FOUO)~~ What words would I have for anybody who might put himself or herself into that category? I would start by pointing out how very fortunate we are to have the opportunity to have a career in an area that is so vital to our nation's well being as to almost defy measuring. I would suggest we focus more on what we might do about helping to attain success and slightly less on what we find distracting. Of course our Agency has challenges and problems today never before encountered. Many are ones over which we have no control as Congress has mandated them. Other sources of irritation to some come from within the building, not that what irritates one necessarily irritates another.

~~(C-GCO)~~ (Ironically, one of our Agency's greatest contributions over the years helped in its own way to bring about a cause of frustration many seem to feel. I'm talking about the valuable work done by NSA in bringing about the demise of the Soviet Union.)

~~(FOUO)~~ Attempts are being made to resolve some of the Agency's problems even as others are emerging. I submit few places one could find employment are devoid of such. The whole point of what I'm trying to say, however, involves what else we have going for us. We have a reason for being found few other places. You don't believe me? Compare your fate with others you know who work elsewhere. I'll avoid making real comparisons; I'll stick with a rather silly hypothetical one instead. I maintain what we're doing is slightly more important and relevant than, say, doing research on finding the best possible container in which to package corn flakes.

~~(FOUO)~~ Promotion rates may have slowed down. Other sources of concern are certainly present. The frustrations involved with a career can't be shed, of course, merely by waving one's hands and wishing them away. They can, however, largely be overcome by a focus on the positive. Be grateful we have a mission whose importance is such we can draw comfort from it simply by turning to it. Am I saying we should therefore turn our backs on the problems we face? Of course not. All I'm saying is we shouldn't dwell on them. Finally, when all is said and done, the greatest reward you likely will ever receive is the one you give yourself upon the realization you gave your very best to the effort at hand.

~~(FOUO)~~ Is this simply the ranting of one who feels incredibly fortunate to have had the career he's had -- particularly from the safe confines of Australia -- as he's about to enter retirement? Perhaps, but I would point out I have been saying the same thing for years. My motivating factor is to do what little I can to raise the spirits of those who might feel the need for it. Our mission -- fortunately for all of us -- is about a thousand times too large to do otherwise. We need for everybody to focus on the job at hand for us to continue doing what we've been able to do for so long.

~~(FOUO)~~ P.S. Back to the topic I first thought of writing about. Would you likely find a PCS tour at DSD rewarding and enjoyable? Do birds fly?

****
//////////

2. ~~(TS-GCO)~~ CALENDAR

(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

Jan 9 [redacted]

Jan 11 Science & Engineering Society Presentation - "Microsensors and Supercomputers", [redacted] Jet Propulsion Labs, (R&E Symposium Center, 1000)

Jan 12 "Real World Applications in Large Scale Combinatorial Optimization", an R55 Seminar, (R&E Symposium Center, 0830-1200) (See Community Service)

(b) (6)

Jan 17 Second Annual Breakfast Affair for Newly Certified Cryptanalysts (BANCC), (Canine Suite, 0800-1000)

Jan 19 Joint CMI-KRYPTOS Talk, "INFOSEC Posture and Threat", by Rick Proto, Chief R, (Friedman Auditorium, 0900)

PLAN AHEAD

Feb 15 Science & Engineering Society Presentation - "Latest Technology in Modeling and Simulation" [redacted] Silicon Graphics, (R&E Symposium Center, 1000)

Mar 14 KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman Auditorium, 1300)

Mar 14 Science & Engineering Society Presentation - "LIGHTING Project for High Speed Data Transfer between Computer Systems", [redacted] NSA Laboratory for Physical Sciences, (R&E Symposium Center, 1000)

Mar 25-29 CARD

May 13-17 ACE 1996 at CCS in Bowie

June 18 KRYPTOS Talk (Subject/Speaker to be Announced), (Friedman Auditorium, 1300)

Sep 17 KRYPTOS Talk (Subject/Speaker to be Announced), (Friedman Auditorium, 1300)

Fall? CONSCRYPT '96, at DSD

Nov 19 KRYPTOS Talk (Subject/Speaker to be Announced), (Friedman Auditorium, 1300)

****
//////////

3. (FOUO) KRYPTOS NEWS

The outgoing Officers of the KRYPTOS Council and 1996 Officers wish everyone a happy and safe holiday season!

(b) (3)-P.L. 86-36

****

a. (U) BANCC Plans Underway

(FOUO) [redacted] is chairing the Second Annual Breakfast Affair

[redacted]

for Newly Certified Cryptanalysts to be held on January 17th. Among those items featured on the menu are -

Crisp Bacon
Sausage
Farmer's Scrambled Eggs
French Toast
Hash Brown Potatoes or Cinnamon Apples
Homemade Biscuits
Coffee and an assortment of Teas
Juice

Sign up and pay $6.00 to one of the following people by Friday, January 12, 1996.

[redacted]

List of Honorees:

[redacted]

(b)(3)-P.L. 86-36

---

4. (U) CACP NEWS

The CACP sends Seasons' Greetings to everyone!

---

5. (U) COMMUNITY SERVICE

a. (U) R55 Seminar

(b)(6)

(FOUO) The Center of Operations Research (R55) has scheduled a seminar on January 12, on the application of large-scale, combinatorial optimization to real world problems. [redacted], Professor of Operations Research from the Post Graduate School at Monterey, will discuss how large scale, mixed-integer programming models have been applied to problems in both the private and military sector. [redacted] will provide a hands-on presentation of the state-of-the-art in combinatorial optimization and associated COTS (Commercial Off-The-Shelf) software, stressing applications -- not theory. The lecture will be provided in four parts:

(b)(3)-P.L. 86-36

[redacted]

1. (FOUO) A 30-minute introduction into the terminology and principles of Large-Scale Combinatorial Optimization.

2. (FOUO) A 60-minute discussion of several military and Fortune 500 success stories. One particular application required more than a million binary variables, yet could be solved on a personal computer using Benders Decomposition Algorithm. Another example application has been used by the Air Force for sortie planning and for justifying billions of dollars in non-nuclear weapons procurement.

3. (FOUO) The next segment (90 minutes) will focus on notoriously difficult problems and recent mathematical advances that have appeared in COTS packages which render these combinatorial models solvable. These solver packages are mated with new, quick-prototyping, algebraic modeling languages opening new horizons.

4. (FOUO) In the afternoon (starting at 1300), [redacted] will provide an informal demonstration of a PC-oriented optimization tool kit that is flexible for quick response modeling. The tools provide ad-hoc report writing capability with a graphical user interface, as well as the ability to build and solve sophisticated problems overnight. [redacted] will then be available to discuss actual Agency problems put forth by the audience at the TSSI level. (b)(6)

(FOUO) Parts 1 through 3 will be provided from 0830 and 1200 in the R&E Symposium Center (seating on first-come basis). Part 4 is intended to be more interactive in nature and will be limited to a smaller audience. Those interested in attending part 4 should reserve a seat by sending a request via e-mail to [redacted]. (b)(3)-P.L. 86-36

****

b. (U) CRYPTOLOGIC ALMANAC

(U) "A View from the Other Side"
(David A. Hatch, Director, Center for Cryptologic History)

(FOUO) Visitors perusing the World War II exhibits at the National Cryptologic Museum are often surprised by the extent the Allies penetrated German and Japanese codes and ciphers. This frequently leads them to ask whether the Axis powers had any success against U.S. cryptographic systems. It is clear that neither Germany nor Japan ever succeeded in breaking into the highest level U.S. machine system, the SIGABA. However, the story is less rosy for systems of lesser grade.

(S) Following World War II, the U.S. Army Office of Military History had former German signals intelligence personnel compile a history of German SIGINT operations against Allied forces during the war. The following are excerpted items from this history, a cautionary tale about American communications security.

(S) The German author noted that up to 1942, military communications by units deployed to the United Kingdom were easily exploited by the Germans. These communications revealed APO numbers, unit designations and abbreviations, and officer promotion lists. American communications revealed to the Germans the activation of units, their training, and impending shipment overseas; unit APO numbers allowed the Germans to follow the units once they reached the European theater. This basic information on the U.S. military stood the Germans in good stead during the rest of the war.

(b)(3)-P.L. 86-36

[redacted]

~~(S)~~ British, and then American, communications security practices were strengthened after the summer of 1942. At the battle of El Alamein, the British captured the entire stock of equipment of the intercept company attached to the German Afrika Corps. This gave them a better appreciation for the SIGINT capabilities of their adversary.

~~(S)~~ Although the Americans adopted better communications security practices after 1942, modeling their procedures after those of the more experienced British, the Germans noted that radio discipline deteriorated rapidly when U.S. troops entered combat. The inexperience of American soldiers, combined with an "abundance of radio sets," tempted communicators to send too many messages in the clear. This provided the enemy with "many clues regarding the tactical situation and U.S. intentions" and allowed them to solve many American tactical cryptosystems. American COMSEC improved as the war continued, but not uniformly. Even when COMSEC was good at senior levels, this was often compromised by poor security measures at lower-level units.

~~(S)~~ Seemingly unimportant messages often provided critical information to the enemy. German intelligence lost continuity on an American airborne unit which had been fighting in Italy. After some weeks, a net in the U.K. -- hitherto unidentified by the Germans -- transmitted a message seeking a soldier against whom a woman in the United States had instituted a paternity suit. The identifying information of this soldier tallied with the missing airborne unit, leading the German SIGINT service to believe it was now stationed in England, readying for the cross-channel invasion. Subsequent analysis of American communications bore out this hypothesis.

~~(S)~~ The German author singled out for criticism American military police communications during the Ardennes offensive (popularly known as the "Battle of the Bulge"). He says that "all established rules were violated," that the German high command obtained complete information on U.S. operations, and he suggested that "given a less unfavorable distribution of forces," the outcome of the battle might have resulted in German victory rather the other way around, given this special knowledge.

****

c. (U) CALL FOR PAPERS: ACE 96

~~(FOUO)~~ The 1996 Annual Cryptomathematics Exchange (ACE 96) will be held 13-17 May 1996 at the Center for Computing Sciences (CCS) in Bowie, Maryland, USA. ACE is the classified community's premier conference for cryptomathematics.

(U) The conference will feature both general sessions (talks of general interest) and specialized sessions held in parallel. Conference proceedings will be published containing abstracts of the general talks.

~~(FOUO)~~ General talks will be 20 minutes in length. They should be summaries rather than detailed presentations, designed for cryptomathematicians who are not specialists in the speakers field of expertise. Additional time may be given during parallel sessions as requested (see below) to provide further details and examples, or to answer questions or conduct discussions. General talks may be classified up to TSC, and may not contain compartmented or source-related material. General talks must be releasable to nationals of the US, UK, Canada, Australia, and New Zealand, and to IDA.

(b)(3)-P.L. 86-36

~~(FOUO)~~ Parallel sessions will feature 20-30 minute follow-ups to the general talks as well as presentations of results not releasable to all attendees. Parallel talks may not be NOFORN and must be releasable to IDA.

~~(FOUO)~~ Those who wish to present a talk at ACE 96 should submit a preliminary abstract to an ACE representative (see below for names). The preliminary abstract should be one or two pages (preferably one) and consist of:

-> Title and Speaker
-> Authors (if joint work)
-> Classification of talk
-> Summary of work, suitable for nonspecialists
-> Request for parallel-session time, if desired.

~~(FOUO)~~ The abstract should be properly classified, including paragraph classifications. The preliminary abstract must be in ASCII form and be e-mailed to an ACE representative by Friday, February 2, 1996. In addition, U.S. personnel should send a hard copy to [redacted] R&E Bldg, along with a Conference Approval Sheet (available from your ACE rep) signed by the speaker's Branch-level management. Australian, Canadian, New Zealand and UK submissions should be made through the appropriate liaison office.

(b)(3)-P.L. 86-36

~~(FOUO)~~ The ACE Committee will select the talks to be given and notify the speakers in late February. Those selected for general talks will be asked to submit full abstracts for inclusion in the conference proceedings. The full abstracts will be up to 8 pages, in PostScript format, and will be due in mid-April.

~~(FOUO)~~ Questions/problems should be referred to your ACE representative:

[redacted]

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) Qualifications: Students should have an engineering or physical science degree. Some familiarity with elementary probability is assumed. A high degree of participation is expected, so that the workshop will be well-tested and critiqued. Only green or gold badge personnel may attend.

~~(FOUO)~~ Instructor: [redacted] is an adjunct NCS faculty member and a recent graduate of the Cryptomathematician Program. He developed this workshop at the request of the Science and Engineering Society. (b)(3)-P.L. 86-36

(U) Enrollment: Space is limited to 30 participants. Because of the lateness of this announcement, please email to [redacted] subject: Dan's workshop, if you wish to attend. You will be notified if you may attend the class on 3 or 4 January 96.

(U) Credit: This should be considered a pilot offering. An NCS course designator has been requested.

(U) If you have any questions about registration or course content, please contact [redacted] (on leave 20 Dec - 2 Jan). Contact [redacted] for questions on course content.

~~(TS-CCO)~~ We have asked the Z Classification Authority for specific guidance on the classification of this workshop. While the course material is derived from unclassified sources, there is precedent for classifying the fact of the Agency's interest in the topic as Top Secret - COMINT Channels Only. (b)(3)-P.L. 86-36

****
//////////

6. (U) TIDBITS

a. ~~(FOUO)~~ IN THIRTY YEARS by [redacted]

MARINE GUARDS.....METAL BADGES.....THE OLD HOSPITAL SITE.....MOVING S FROM NEBRASKA AVENUE.....SEPTIMUS.....CAROL'S HANDS IN ALAN'S POCKETS TRYING TO PASS THE PLATE.....THE PUEBLO.....THE LIBERTY.....DESERT STORM.....KATCINA.....CLASS 26 OF THE ISPGC WITH "THE GURU".....FRANK AND MARY.....BOB AND DIXIE.....DICK AND HELEN.....JUDITH.....SPICE... ...AKIF.....THE BIRTH AND DEATH OF CK-600.....BATTLES OF LAUREL, FREDERICK, AND ANNAPOLIS.....CHRISTMAS GAMES AT CATHY'S.....THE HANTMAN CASE..... THE KRYPTOS SCULPTURE.....TDY'S TO EXOTIC PLACES.....2A AND 2B..... Z GROUP AND THE "GANG OF EIGHT".....WINDSONG AND LE CHANSON.....WARS IN THE MIDDLE EAST.....PROJECT KAY.....5500, 6600, 7600, AND SIGN-UP SHEETS .....THE ACES.....SKYHIGH.....CARTER, GAYLER, PHILLIPS, ALLEN, INMAN, FAURER, ODOM, STUDEMAN, AND MCCONNELL.....MISS NSA.....ITB.....DEG... ...H-460 AND THE CAST FROM "THE AVENGERS".....GUPPY AND PAPER TAPES..... SLIP STICKS.....G4 PARTIES.....SOFT PORN ADVENTURE.....TRIVIAL PURSUIT .....THE HOSTAGE CRISIS.....KAL 7.....CROSS HATCH PAPER AND COLORED PENS.....IC'S ON THE FREIDMAN CALCULATOR.....JIM SNOWBOUND FOR FOUR DAYS.....BLACK CLOTHS.....RNG'S.....64K PC'S.....MANAGEMENT GRID,

(b)(3)-P.L. 86-36

[redacted]

Doc ID: 6823799

MBO, TQM, ET AL.....IBM CARDS AND METAL TRAYS.....MEN IN TIES AND WOMEN IN DRESSES.....MATERIAL INSPECTIONS.....HALLOWEEN AND BORIS HUNTINGTON .....LIZABETH SCOTT.....HENKEL HAM THROUGH-THE-GARDEN FOR $.80..... SMOKING AT THE DESKS....."THE BRIG".....CONFIRM.....

****

b. (U) BOOK REVIEW by [redacted] (b)(3)-P.L. 86-36

Text Compression, by Timothy C. Bell, John G. Cleary, and Ian H. Witten. (Prentice Hall Advanced Reference Series, Prentice Hall, Englewood Cliffs, New Jersey, 1990.)

(U) The authors present a wide-ranging treatment of a variety of topics in the data compression field. Particularly interesting topics included an investigation of natural language characteristics and practical comparisons of coding schemes including Huffman, Shannon-Fano, and Arithmetic Coding. Throughout the book a host of clear explanations and numerous examples are provided, while theoretical, mathematical discussions are generally relegated to appendices or separate note sections. The overall text is quite readable, and provides a strong foundation for further study of the topic. While not designed to serve as a "how-to" guide, the book successfully provides a serious treatment of the underlying principles of text compression.

(U) Text compression involves finding ways to represent text with symbols using fewer bits than the original characters required. The process should be reversible; that is, the new representation can be uncompressed in order to regenerate the original text, and it is usually important that the original can be recreated exactly, not just approximately. This sets text compression apart from other types of data compression such as voice or image compression, where some loss of quality may be acceptable if significant compression can be achieved.

(U) The authors suggest that text compression is essentially text prediction. If we can predict the next character, word, or phrase in text, we need not transmit it, and as a result can transmit the message in fewer symbols than originally required; i.e. we have compressed the message. All predictions for the next character, word, phrase, etc. can be based on a model of the message. The task of finding a suitable model for text is an extremely important problem in compression. Once predictions (probabilities) are determined, they are processed by an encoder that turns them into binary digits to be transmitted.

(U) The idea of separating the compression process into two parts -- an encoder and a separate model that passes information to it -- is a major advance in the theory of data compression. The prediction, in the form of a probability distribution over all messages, is supplied by the model. The encoder is given the prediction, along with the actual message that occurs, and constructs a compressed representation of the actual message with respect to the probability distribution. Note the encoder does not need to know where the predictions come from, and as a result can work with many models. According to the authors, the issue of constructing an encoder has been completely solved, in a way that is as close to optimal as practically possible. However, the problem of constructing models for different kinds of data is more artistic than mathematical, and cannot be said to be solved in any definitive way. A majority of this book is dedicated to discussion and comparison of

[redacted] (b)(3)-P.L. 86-36

alternative modeling strategies.

(U) One pervasive theme throughout the book is the effectiveness of using adaptive models over static models. An adaptive model is one that changes as the message is encoded so the model better suits the message. After a lengthy mathematical comparison between adaptive and static models, including a discussion of "conditioning classes" (how the text is to be partitioned) and the "zero-frequency" problem (how to represent the probabilities of symbols that never appear in the text), the conclusion is drawn that, in a wide range of circumstances, adaptive models can only be slightly worse than any static one, but static models may be arbitrarily worse than adaptive models if the text is statistically different from the model being used. Thus the authors support adaptive techniques over static in almost every case.

(U) In addition to an extensive discussion of modeling, practical algorithms for an encoder are also presented. The basic compression problem can be stated as follows: Given a probability distribution that is assumed to govern the choice of the next symbol, and the symbol that actually occurs, find an algorithm to generate bits that specify the symbol to a decoder which is aware of the same distribution. The best known method for coding with respect to a probabilistic model is Huffman Coding. While this method is often touted as the best possible technique for reducing the encoded data rate, the authors disagree. A more recent development, Arithmetic Coding, is presented as superior in almost all respects. Arithmetic Coding represents information at least as compactly, and sometimes considerably more so than Huffman Coding. Arithmetic Coding encourages a clear separation between the model for representing the data and the encoding of information with respect to that model. It accommodates adaptive models easily, and is computationally efficient. In their enthusiasm for the technique, the authors go so far as to provide a full software implementation for Arithmetic Coding in the C programming language in an appendix to Chapter 5.

(U) Each of the coding schemes discussed strives to give high-probability messages short codes and low-probability ones longer codes. On occasion, Shannon-Fano Coding will assign a longer code to a more probable message than it does to a less probable one. Huffman Coding, however, can be shown to generate codes that produce the shortest possible average code length given the message set's probability distribution. However, in both of these coding schemes, every symbol in the alphabet must occupy an integral number of bits in the encoding. Arithmetic Coding disregards this restriction, thereby coding more efficiently. It actually achieves the theoretical bound for compression efficiency. The technique is considerably more intricate than either Shannon-Fano or Huffman Coding, and a full treatment with a computational example is provided. Essentially, a message is represented by an interval of real numbers between 0 and 1. As the message becomes longer, the interval needed to represent it becomes smaller, and the number of bits needed to specify that interval grows. Successive symbols of the message reduce the size of the interval based on the symbol probabilities generated by the model. The more likely symbols reduce the range by less than the unlikely symbols, and hence add fewer bits to the message.

(U) After an exhaustive treatment of Arithmetic Coding and other statistical techniques, the authors move on to discussion of the other class of text compression techniques, dictionary coding. These techniques specifically include the Ziv-Lempel (LZ) family and several

(b)(3)-P.L. 86-36

9/23/2010

variations are presented. While statistical methods use probability estimates for each character and choose a code based on the probability, dictionary coding achieves compression by replacing groups of consecutive characters with indexes into some dictionary. The dictionary is a list of character groups that are expected to occur frequently. Indexes are chosen so that on average they take less space than the character groups they encode, thus achieving compression. A lengthy comparison of various dictionary methods is presented.

(U) So which compression method is best? The answer is simply, "it depends". It is difficult to make direct comparisons between statistical and dictionary schemes, and a number of issues must be evaluated: models used, speed of compression, amount of compression achieved, and memory requirements. In order to give some practical comparison of popular methods, a corpus of various types of text, including fiction and non-fiction books, object code, C programs, technical papers, and electronic mail messages was used, and a number of graphs are provided to show how each technique fared against each type of text.

(U) As a result of their extensive presentation, Bell, Cleary, and Witten have made a murky subject accessible to the layman as well as the earnest student. "Text Compression" presents the facts and underlying principles in a usable fashion for readers of all levels, and this reference deserves a place on the shelf of any serious student of compression techniques.

****
//////////

7. (U) PUZZLES AND PROBLEMS

~~(FOUO)~~ This month we bring you a present from our KRYPTOS Chapter at Cheltenham, courtesy of [redacted] For solvers here, the closing date is the 19th of January. The first person to provide the correct solution, OR, that with the highest score, to [redacted] our Puzzle Editor, will be treated to an Ice Cream Sundae by the Newsletter staff. The names of all those submitting solutions will be featured in the February newsletter.) (b)(3)-P.L. 86-36

~~(FOUO)~~ (Note from GCHQ: one or two questions have a rather British theme, and one depends on spotting the names of two CC (Cheltenham Chapter) members (both contained in the opening blurb, so that needs to be retained).

~~(FOUO)~~ [redacted] have again put their warped minds together to produce the 1995 Kryptos Kristmas Kwiz, designed to keep you from all the things you OUGHT to be doing (work, Christmas shopping, etc.). Last year there were several quizzes running over the Christmas/New Year period, so this year we're getting in early! (b)(3)-P.L. 86-36

(U) As before, some questions are more difficult than others, and so each question has an associated Warp Factor. For Factors greater than 1, points may be given for a nearly-correct answer or even a gallant effort, so enter something on the answer sheet even if you're not sure. If your answer is better than ours, you may receive bonus points.

~~(FOUO)~~ Note than [redacted] and so thinks

[redacted]

that A is the first letter of the alphabet; [redacted] works in H, so thinks that A is the zeroth letter of the alphabet. But we're not going to tell you who originated which questions..... On the other hand, there are a few hints which are designed to be helpful. (b)(3)-P.L. 86-36

~~(FOOL)~~ Chambers Twentieth Century Dictionary will be taken as the authority for what constitutes a "word", and has been used to provide definitions. Unless otherwise stated, "words" do not include proper nouns or entries which contain punctuation (hyphens or apostrophes). [Note: North American solvers may use Webster's Ninth New Collegiate Dictonary if Chambers is unavailable. Solvers "down under" are likewise welcome to choose an alternate reference held as an authority by their respective agency.]

1. (U) Write down your name, section and room number. (1)
(This way EVERYONE gets AT LEAST 1 point!)

2. (U) Keys may be produced by "numbering off" a keyword or phrase - replace the first A by 1, the second by 2, etc. Given the key, it can be quite difficult to recover the keyword. One method works reasonably well with longish (10-12) words containing letters which are fairly evenly spaced in the alphabet: replace 1 by A, 2 by C, 3 by E, etc. and see if you can pull the word out of a matrix containing this sequence plus 1-offs, 2-offs, etc. For shorter words (6-9 letters) replace 1 by A, 2 by D, 3 by G, etc. Define "distance" as the sum of the differences between each letter of the generated stream and the corresponding letter in the keyword. Example:

keyword:	L	U	M	B	E	R	J	A	C	K
key:	7	10	8	2	4	9	5	1	3	6
stream:	M	S	O	C	G	Q	I	A	E	K
diffs:	1	2	2	1	2	1	1	0	2	0

distance: 12

(a) what 7-letter word has the smallest distance? (1)

(b) what 10-letter word has the smallest distance? (1)

(c) what 11-letter word has the greatest distance? (2)

3. (U) The following words relate to members of families: identify the surname and initials of each member of the family (noting that different members of a family may have different numbers of Christian names):

(a) DISMOUNT, BAY, FUNGUS, SHINING, STRIVE, SOARING, LOAD, TERROR, HILL, CHESSMAN and AMUSING (1)

(b) CONTEND, HAGGLE, PILFERER, WITCH-FINDER, SWIFTER, HEART, OSIER (1)

and a slight variant,

(c) START, INDULGENT, BESTOWAL, NOTING, FLOOR FABRIC, THEFT, WHISTLING, APPAREL, EAGER (2)

4. (U) What have the following in common: BLOOMERS, BOYCOTT, DIESEL, LYNCH, SILHOUETTE? (1)

5. (U) If "Smith and Jones" in Great Britain correspond to "Johannsen and Andersen" in Sweden and "Chang and Wang" in China, what are the equivalents in Korea? (1)

(b)(3)-P.L. 86-36

[redacted]

Doc ID: 6823799

6. (U) What have the following in common: John Bunyan's "Pilgrim's Progress", Miguel de Cervantes' "Don Quixote", Adolf Hitler's "Mein Kampf", Marco Polo's "The Travels of Marco Polo" and Sir Walter Raleigh's "History of the World"? (1)

7. (U) What have the following in common: Willy Brandt, Paul Cezanne, Leonardo da Vinci, Alexander Hamilton, Sophia Loren, Ramsay MacDonald and Richard Wagner?

8. (U) (a) What was the series that came between Mercury and Apollo? (1)

(b) How many men have landed on the moon? (1)

(c) What was the name of the dog which the Russians sent into space aboard Sputnik 2 in 1957? (1)

9. (U) Many words which are 3n long can be broken down into n 3-long words, e.g. FORGOTTEN = FOR + GOT + TEN. Reconstruct the 9 words which produced the following list of 3-letter words:

AGE AGE AGE ANT ANT CON CON CON DIT ERA ERS FED HER HOG IMP
ION ORT ORT ORT ORT PAR PER RAP REP REP SON SON SON TED (1)

10. (U) Where does "CANE" fit in the following list (read across lines in order):

BET	MAX	ALLEY	CLEVER	RING	BOX	BAT
LAWN	MEN	WING	HOUSE	THUMB	PROBLEM	BRER
DION	CLUB	EIGHTH	STICK	CLIENT	BUCKET	PINK
FACTOR	SLIM	BACHELOR	BUILDER	CLEAR	MOON	LATELY
LOT	QUESTION	CHICKEN	PLUG	CIRCLE	TYRANNOSAURUS	BOAT
UNION	BEAR	TENOR	GENTLE	PACK	TABLE	CYCLIST
COURT	POOL	BISCUIT	RUS	INCOME	POP	POOH (6)

11. (U) What is the next in the series: Chariots of Fire, Gandhi, Terms of Endearment, Amadeus, Out of Africa, Platoon, The Last Emperor, Rain Man? (1)

12. (U) What is the next number in the following sequences:

(a)	1	1	2	3	5	8	(1)
(b)	-1	-1	1	5	11	19	(1)
(c)	2	1	0	17	118	513	(1)
(d)	0	-6	-21	-40	-5	504	(1)
(e)	-2	-5	-11	-17	13	295	(2)

13. (U) [Unfortunately, the first part of this question got lost, but see if you can solve it anyway.] We had to dismiss our insolent maid, Diana. She said "A house is nothing but a house", at which we got exasperated. She would say "Oh, I ought to do some washing tonight", but she rarely did. She often bought small packets of detergent when large, or giant-sized, packets would have been more economic. And she dressed carelessly: more than once the words were spoken "Tuck your blouse in, Diana". Dismissal became a foregone conclusion.

14. (U)

CDHHDPJ	SWTTWON	TXLQU	*******	GFHIE	QDSTPQW
****	BZTDX	XWCPQW	FCSOIC	ZSYKDS	IWYGOIC
VAGWF	RPBCZ	QOVSA	AYUMWY	PUEJCU	DCUBKDS
IKRYP	DMQUO	OEXNSE	JPQU	XHDAPVXGT	NPJXY
STPQHXY	YGOITFU	LONFU	??????? AND ????		

(b)(3)-P.L. 86-36

(a) One could make a case for ******* and **** appearing as plain text. What are they? (1)
(b) What are ??????? and ???? (2)
(c) Given that the hatted alphabet starts with C, how was it generated? (2)

15. (U) Determine the rule by which the alphabet has been divided into two parts:-

(a) AHIMOTUVWXY / BCDEFGJKLNPQRSZ (1)
(b) ABCEHKMOPTXY / DFGIJLNQRSUVWZ (1)
(c) AIKMOPRSTWYZ / BCDEFGHJLNQUVX (1)
(d) AEFHIJLPRSUVW / BCDGKMNOQTXYZ (2)
(e) ACDEKMNOUXYZ / BFGHIJLPQRSTVW (3)

[If you don't see the last one within a few minutes, you might feel that it's an unfair question] (b)(3)-P.L. 86-36

17. (U) What is one hundredth of a kwatcha (or kwacha)? (1)

18. (U)

BRITAIN	-3	-1	(1,2)	1-	2-	2-				SPAIN	
ECUADOR	-5	-4	-2	(1,2)	(3,4)	(1,4)	1+			PERU	
GERMANY	-7	-4	(2,3)	(3,4)	(4,5)	+5	1-	5+	5+	FRANCE	
GREECE	-6	-5	(1,3)	(2,3)	2+	2+				?	(1)
?	-2	(1,3)	(3,4)	4-	4-					IRAQ	(1)
?	-8	-7	(2,5)	6-						?	(2)

19. (U) The following list of words can be divided into two sets, of equal length, on the basis of another word:

awe	body	day	fear	hand	how	lone
one	thing	tire	what	where	whole	win

What is the other word? (1)

20. (U) A little crossword (deduce the grid):

(b)(3)-P.L. 86-36

1a. Repose in which there's tranquility?
5a. Always in the middle of a river.
6a. Remove a girl's head.
7a. Commonly half, not more.

1d. "The River's Return"? Try again!
2d. Incomplete result, indeed.
3d. Betray a Scots personality.
4d. Oddly, three by three. (1)

21. (U) "Identity" quizzes have become popular recently. These comprise a list of numbers, each associated with the initials of an object connected with that number, e.g. 24 H in a D (hours in a day). This is much too easy for Kryptos types. You are asked to identify the six numbers associated with the following initials, which will allow you to predict the seventh (appropriately).

(1) M and HD (2) F in an OP (3) S of a L's T
(4) P in a G (5) D in a WW (6) W of the W

What is the next number? (1)

22. (U) (a) What do Victoria Holt, Philippa Carr and Jean Plaidy have in common? (1)
(b) By what name is Cecily Isabel Fairfield better known? (1)
(c) Which of Daphne du Maurier, James Michener and Robert Heinlein follows Barbara Cartland, John Ernest Steinbeck, George Orwell, Graham Greene, H E Bates and Catherine Cookson? (1)

23. (U) In which country is June 24 the Anniversary of Currency, Promulgation, Constitution and Day of Fishers? (1)

24. (U) Each of the following is the name of a province, state, county, region or district of a country: SOMOGY; MAT; GREVENMACHER; RUGGELL; VORARLBERG; AKERSHUS; RIBE. The first letter of each country, in order, spells the name of a county in a different country. Which? (1)

25. (U) (i) Each of 15 words is defined below. Each letter of each word is to be replaced by a digit (you must work out the digit-for-letter substitution) to give a series of numbers with an obvious connection.

(a) (coll) a lavatory (b) shelter (c) scoop up with the tongue
(d) (dial) girl (e) any fish of the species Apodes (f) tree
(g) (slang) partner (h) mislay (i) used to scare away fowls etc
(j) obstruct (k) (coll) interjection for God (l) relieve
(m) mince (n) fellow (o) (slang) smart

Find a 5-letter word with the same property. (2)

(ii) A similar problem, but with an added dimension:

(a) concerning (b) past (c) (Scot) to cause, compel
(d) Syriac or Coptic bishop (e) schools of whales (f) ventilated
(g) jellies prepared from seaweeds (h) hollow cases containing explosives, etc.

(b)(3)-P.L. 86-36

What is the next word in this series? (1)

26. (U) Write down the name of the composer:
(a) whose first symphony was referred to as "Beethoven's 10th";
(b) whose first, but unnumbered, symphony is now referred to as his "Symphony No. 0";
(c) whose symphonies 8 and 9 are often heard, his 7th never;
(d) who wrote a full-scale, unnumbered (but named), symphony between his 4th and 5th;
(e) whose 8th is called "the symphony of a thousand";
(f) who didn't write his "own" 37th;
(g) whose symphonies originally numbered 1-5 were renumbered 5-9 half a century after his death;
(h) who claimed to have completed his 8th symphony but apparently never set pen to paper;
(i) who wrote 12 symphonies as a boy before writing his "First"?

The letters at positions 1, 7, 6, 1, 3, 2, 2, 4 and 3 respectively spell out the name of which other composer? (1)

27. (U) Some more series:

(a) 1 4 10 17 27 40 54 71 100 ? (1)
(b) E D C F T ? Y H N J I (1)
(c) 1 4 9 10 19 24 31 40 51 64 79 90 ? (1)
(d) A H A L U H E T A L E L ? (2)
(e) ? 30 42 54 66 78 90 144 259 (1)
(f) ? 30 42 54 66 78 90 102 114 (1)
(g) 7 14 19 29 40 44 52 59 73 83 94 (1)
(h) 187 243 267 351 366 474 586 826 922 958...? (28th element) (1)
(i) 18 25 28 34 35 37 41 44 ...? (44th element) (1)
(j) 1010001 100111 21301 20141 15041 ...? (14642nd element) (1)
(k) T B O N T O E H T S H ? (1)

28. (U) The letters of the alphabet have been given scores according to two particular rules. For each rule determine what score N should have.

Rule 1 1: ET 2: AIM 3: DGKORSUW 4: BCFHJLPQVXYZ (1)
Rule 2 4: EGKLMPXYZ 5: ABDHIORT 6: JQSVWY 7: CFU (1)

29. (U) (a) What is the shortest word that can legally be played in a game of Scrabble, but which can never appear on a Scrabble board? (1)

(b) In Scrabble, the following letters score 1: AEILNORSTU. What is the longest word consisting only of letters scoring 1? (1)

(c) The following letters score more than 1: BCDFGHJKMPQVWXYZ. Which word contains the longest unbroken sequence of letters which score more than 1? (1)

30. (U) Define the "area" of a crossword as the number of squares in the square/rectangle that the whole grid needs. Compose a crossword which contains all the letters of the alphabet and has the smallest possible area. The crossword grid should be a normal one, with all strings of adjacent letters forming words (e.g. daily Times, Mail, Independent, etc.) rather than one in which bars are used to separate letters which do not form words (e.g. Listener, Saturday Independent, etc.). (3)

31. (U) Twelve words have been enciphered using a substitution system. Decipher the words and then, using the same system, encipher a 6-letter

(b)(3)-P.L. 86-36
9/23/2010

word which sums up the 12 words.

27437, 728787, 436464, 226237, 530, 84740, 54272, 7207640,
72447727487, 226742076, 20827487, 647237. (2)

32. (U) Who, or what, are, or were, MERCHED and DYNION? (1)

33. (U) There's a game of cards in which players take it in turn to make a rule about whether or not successive cards should be accepted or rejected, and the other players have to determine the rule. You are to determine the rules for each of the following 3 sequences (O=accept, X=reject), and complete the sequence (NB T=10):

4A984J6Q44967625AT3783KK75T375Q28J5A2Q93T8TQ26JJAK9K
DHCCCCDCSHDHSSDCDHDDDHCHHDCSCSDSHSHSCHSCDSSSHCHDCDHS

(a) OXOOOOOOOOOOOOOOXOOOOOXOOOOOOOOXXOXOXXOOXXXOOX..... (1)
(b) OXXOXXXOXOXXOXXXOOXXOXXOOXXOXXXOXXXOXOOXXXOXXXO..... (2)
(c) OOOOXXXXXOOXXOOXXXOXXOOXXXOXOOXXOXXOOOXOXXXXOXO..... (3)

34. (U) (a) Who led the army which won the battle of Stirling Bridge? (1)
(b) Who is mourned in "In Memoriam"? (1)
(c) Who had a Number 1 in 1960 with "Only the Lonely"? (1)
(d) Who partnered both Hart and Hammerstein? (1)
(e) Who wrote "Book of Nonsense" in 1846? (1)
(f) Who married Vivien Leigh in 1940? (1)
(g) Who won the Nobel Peace Prize in [unfortunately the year was obliterated by a coffee spill...] (1)

(U) KRYPTOS KRISTMAS KWIZ

1. Name: Section: Address:

2. (a) (b) (c)

3. (a)

(b)

(c)

4.

5.

6.

7.

8. (i) (ii) (iii)

9.

10.

11.

(b)(3)-P.L. 86-36

12. (a) (b) (c) (d) (e)

13.

14. (a) (b)

(c)

15. (a)

(b)

(c)

(d)

(e)

16. (a)

(b)

17.

18. (a) (b) (c) (d)

19.

20. 1a 5a 6a 7a
1d 2d 3d 4d

21.

22. (a)

(b)

23.

24.

25. (i)

(ii)

26.

27. (a) (b) (c) (d) (e) (f)

(g) (h) (i) (j) (k)

28. 1. 2.

29. (a) (b) (c)

30.

(b)(3)-P.L. 86-36

8. (U) EDITORIAL CORNER

~~(FOUO)~~ BEST WISHES TO [redacted] (b)(3)-P.L. 86-36

~~(FOUO)~~ [redacted] a member of the 'Tales of the KRYPT' Editorial Board, is resigning from the Agency at the end of December to join her husband who is retiring at the same time. The 'Tales of the KRYPT' Editorial Board would like to thank [redacted] very much for her loyal support and creative and insightful contributions to the CA community newsletter. It has been a pleasure for each of us to work with [redacted] We wish her all the best!

~~(FOUO)~~ REMINDER: Submissions for the February issue are due by January 26th. PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION-MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted] (b)(3)-P.L. 86-36

[redacted]

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2, DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR" DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

(b)(3)-P.L. 86-36

[redacted]

9/23/2010

CONFIDENTIAL

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:19
(U)PE EXTERNAL PAGE

THE CLASSIFICATION OF THIS NEWSLETTER IS CONFIDENTIAL

****
* TALES OF THE KRYPT *
****
February 1996

(b)(3)-P.L. 86-36

//
****

(FOUO) TABLE OF CONTENTS:

1. (U) CA Perspective

2. (U) Calendar of Events

3. (FOUO) KRYPTOS News

4. (FOUO) Word from the CACP

5. (U) Community Service

6. (U) Action Line

7. (U) Problems and Puzzles

//

1. (S) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature [redacted] the immediate Past-President of the KRYPTOS Society, and the current Chairman of the Cryptanalysis Career Panel. This is the address given at the Second Annual Breakfast for Newly Certified Cryptanalysts last month.

****

(U) Today's breakfast, honoring you who have been certified in Cryptanalysis during 1995, is in some sense like a commencement exercise. Certainly it is a time for celebration and the CA community gathers very consciously to say that what you have accomplished is important. It is important for you, for your career, in that it opens doors that would not otherwise be open. It is important for the CA community in that it is a significant step allowing us to call upon you to fill more senior leadership roles in meeting the challenges that cryptanalysis faces. And so it is appropriate to pause and recognize you and to say what everybody in this room believes: that this is GOOD; that this is healthy, healthy for CA and healthy for you; and it's a cause for special recognition.

(U) It occurred to me that you recently professionalized will find yourself in an interesting position over the next few years, because CA is in a time of transition. The reason, of course, is that the targets are changing; they are changing because the technology is changing; and all of that change is accelerating. None of this is a surprise to any

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

of you. In fact, there has been a strong grass roots effort across CA (which, I believe, has been effectively harnessed by the previous CA Career Panel) to get us to respond to the shifting playing field we find ourselves on. All of that effort is being played out now in adjustments to the CA certification criteria and extensive changes in formal CA training which will be taking place over the next few years. And so the "interesting" position you will find yourselves in is that you will see the CA community (rightfully) proclaiming a cryptanalyst to be something significantly different from what you have just been certified to be. Don't you find that "interesting"? It's like you aimed at a target and the target moved, quite a bit.

(U) If you think about it, though, it's really no different than where NSA has always found itself, that is, always attuned to change, always in need of ongoing development and education. Only now the fire is turned up higher. However, lest you feel persecuted, let me assure you that

1) you are not alone; the burner is turned up for all of us; we all need to acquire this new knowledge; and

2) (and this refers back to the accelerating pace of technological change) we can't afford to delay; we (all of us) can't afford not to jump on the education train; and, corporately, we must rev up our CA education so that it evolves and keeps pace with the cryptanalytic challenges we are facing.

(U) Some of you, I know, are right in the thick of these developments - some of you have, of your own accord, learned what has been necessary to resolve the complications introduced by the new communications technologies. You are accomplishing things that would astound the outside world, the Baltimore Sun notwithstanding. We will be calling upon you, because the CA community needs to solve its own education problem (and, as an aside, the lion's share of this task falls to Z Group). Meeting this challenge is not only a necessity but also a great opportunity. The challenge is before us; we have the resources to do this thing right; and we can only gain by doing so.

(C) I would like to make one other point of encouragement. About a year ago, Tom Lessard, concerned about Z's continued technical health, challenged Z's cryptanalysts to become proficient in the diverse areas that make Z successful:

- collection, field processing and signals analysis
- research, diagnosis and attack development
- exploitation
- special compartmented activities
- overseas and other external assignments
- staff positions
- leadership positions.

(U) In light of Tom's challenge, in light of the increasing importance of the Tech Track (and I hope all of you realize how much the Tech Track will be affecting your careers), in light of the mission-driven need for more and more knowledge, it is crucial for all of us to take more conscious control of our career paths and ensure that gaps in experience and knowledge are filled. I encourage you to do that.

(U) I encourage you to be a part of gaining experience and part of passing on experience. Be part of the process --- or I should say,

"Stay part of the process" because what you have accomplished which culminated in certification this past year shows that you already are part of the process; you are "engaged". And I salute you for being engaged in keeping Cryptanalysis, the core discipline here at NSA, vibrant and successful.

(U) So it is up to you --- to be aware, to take control, and to make things happen, for yourselves personally and for this discipline of ours, Cryptanalysis. Congratulations on your certification. All of us in this room are proud to have you as colleagues.

//

2. CALENDAR (U)

Feb 15	Science & Engineering Society Presentation - "Latest Technology in Modeling and Simulation" [redacted] Silicon Graphics (1000 R&E Symposium Center) (b)(6)
Feb 20	Mardi Gras Celebration, a KRYPTOS/CMI event, Last Chance Saloon, Columbia, 5:30 to 7:30 P.M.

PLAN AHEAD

Mar 14	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)
Mar 14	Science & Engineering Society Presentation - "LIGHTING Project for High Speed Data Transfer between Computer Systems", [redacted] NSA Laboratory for Physical Sciences (1000 R&E Symposium Center)
Mar 25-29	CARD, at CCS (b)(3)-P.L. 86-36
May 13-17	ACE 1996 at CCS in Bowie.
May 21-22	CA PQE
May 30	MATHFEST '96 and CMI Banquet
June 18	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)
Sep 17	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)
Fall?	CONSCRYPT '96, at DSD
Nov 19	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)

****
//

3. ~~(TOUO)~~ KRYPTOS NEWS

a. ~~(TOUO)~~ BANCC a Huge Success (b)(3)-P.L. 86-36

[redacted]

(U) Jointly sponsored by the KRYPTOS Society and the CACP, the Second Annual Breakfast for Newly Certified Cryptanalysts (BANCC), was held in the Canine Suite on 17 January. Almost 90 people attended to recognize those who were professionalized in the last year. [redacted] and her committee did an outstanding job in putting this together!

(b)(3)-P.L. 86-36

(FOUO) The new cryptanalysts honored were: [redacted]

b. (FOUO) Membership Drive Underway

(FOUO) The KRYPTOS Society needs new members. Join between February 1st and February 16th and you will be entered in a drawing to win one of 50 KRYPTOS coffee mugs. Dues are $5.00 per year. This money is used to purchase gift certificates for speakers, to pay for the Literature and Distinguished Member awards, and to subsidize the cost of the annual luncheon for members who attend.

(FOUO) To join, please complete the attached application, and submit it with your $5.00, to one of the KRYPTOS board members listed below:

[redacted]

(b)(3)-P.L. 86-36

(U) The drawing will be held the week of February 20th, and the winners will be notified ASAP afterwards. Please join KRYPTOS now, and assist the officers and current members in promoting the science of cryptanalysis throughout the Agency.

**** KRYPTOS MEMBERSHIP APPLICATION DUES: $5.00 (Annually)****

MEMBERSHIP YEAR: 1996 ( ) NEW ( ) RENEWAL

NAME:_____ DATE: _____

SECURE PHONE: _____ NON-SECURE: _____

[redacted]

(b)(3)-P.L. 86-36

ORG: _____ BLDG: _____ ROOM NR. _____

SID & HOST: _____

INTERESTED IN CHAIRING A COMMITTEE? ____YES ____NO

INTERESTED IN WORKING ON A COMMITTEE? ____YES ____NO

CHECK COMMITTEES OF INTEREST TO YOU:

____ CRYPTANALYTIC LITERATURE ____ MEMBERSHIP

____ DISTINGUISHED MEMBERS ____ PUBLICITY ____AWARDS

____ PROGRAMS ____ NEWSLETTER ____ RETIRED MEMBERS

****

c. (U) Joint Mardi Gras Festivities Planned

(~~FOUO~~) KRYPTOS and CMI will be celebrating Fat Tuesday at the Last Chance in Columbia. Come enjoy a couple of hours after work with your colleagues and the Last Chance's wide selection of drinks & great appetizers!

(U) The party room is reserved for Tuesday February 20th (the day after Presidents' Day) from 5:30 to 7:30.

(U) The cost is $5.00 per person to cover the price of appetizers (listed below). If you would like to attend, please sign up early so that we can better judge the quantity of appetizers to order.

(U) The appetizers provided include Potato Skins, Buffalo Wings (mild and spicy), Beer Battered Mushrooms, Buffalo Meatballs (mild and spicy), Nachos and Cheese, Cheese Quesadillas, Onion Rings and Garlic Bread au Gratin. Any drinks you buy will be extra. Sign up today!!!

(~~FOUO~~) Please contact one of the following people in order to sign up:

[redacted] (b)(3)-P.L. 86-36

****

//

4. (U) CACP NEWS

a. (U) New Certification

(b)(3)-P.L. 86-36

[redacted]

~~(FOUO)~~ [redacted] has just been newly certified as a cryptanalyst.

b. (U) Announcements

(U) The CA PQE will be on 5/21 and 5/22 (only two days this time rather than three). Look for updates to the CA Computer Requirement next month.

c. (U) GOLD BUG AWARD

(b)(3)-P.L. 86-36

(U) The Cryptanalysis Career Panel is currently accepting nominations for the Gold Bug Award and the Gold Bug Team Award. The Gold Bug is an honorary award created by the Cryptanalysis Career Panel in 1982 to recognize outstanding technical excellence and achievement in cryptanalysis. An individual or a team may receive the Gold Bug Award. While there is no particular time of year that the award is given out, the CA Career Panel encourages all supervisors who have an employee or employees who might merit this distinction to submit their names and a description of their accomplishment to the panel by COB 1 March 1996. There is no specific format for the nomination - simply describe the achievement in narrative form and send through normal administrative channels via regular office memo to the CA Career Panel, H111, OPS 2B room 3036D. Further questions may be directed to the Panel at h111@nsa or [redacted]

//

5. (U) COMMUNITY SERVICE

a. (U) CA Technical Track Review Panel (TTRP) Succession Plans

~~(FOUO)~~ The CA TTRP, which has been operating for over two years, has a number of members who are due to rotate off, and this will lead to a number of vacancies. The TTRP has begun to identify a process for selecting people to serve in this capacity, and is interested in including input from the Z technical workforce in its deliberations. At a minimum, all nominees should hold either a Senior Member or a Master level title in CA. If you would like to volunteer to be considered, or if you would like to nominate an individual for such consideration, please notify [redacted] or [redacted]

b. (U) Former Agency Deputy Director Died

(b)(3)-P.L. 86-36

(U) Dr. Louis W. Tordella, a former top official of the National Security Agency, died of cancer on 10 January 1996 at the age of 84. Dr. Tordella was a pioneer in the science of cryptology and rose to the position of Deputy Director of NSA, a position he held for sixteen years, longer than any other official at NSA.

(U) Dr. Tordella was born in Garrett, Indiana, in 1911 and grew up in the Chicago environs. He displayed an early affinity for mathematics and obtained B.S., A.M., and Ph.D. degrees in the 1930s. The outbreak of World War II found him teaching mathematics at Chicago's Loyola University.

[redacted]

(U) He volunteered for the Army, but the recruiter told him that the Army would draft whomever they needed. So Tordella made contacts in the Navy, and he was brought aboard as lieutenant junior grade in 1942. He went directly into cryptologic work for the Navy's codebreaking organization, OP-20-G, where he worked on the German Enigma cipher machine. He was one of a team of brilliant mathematicians who designed the "bombe," a wartime machine used to decipher the keys on the Enigma. He finished the war at OP-20-G collection stations on the West Coast, at Bainbridge Island, Washington, and Skaggs Island, California.

(U) After the war, Tordella stayed on with the Navy, and in 1949 he joined the newly created Armed Forces Security Agency (AFSA), an early attempt to achieve service unity in the business of cryptology. He was a key figure in devising policy for the new agency and for its successor, the National Security Agency, which emerged in 1952 to replace AFSA. Although a Navy man, Tordella readily grasped the advantages of unification, and he pushed the concept forcefully in the early years.

(U) Tordella's career at NSA brought him to the very front rank of cryptologists. On the technical side, he was an early advocate of the use of computers for cryptologic work, and he helped to cement a close working relationship with a new computer firm, Electronic Research Associates, which eventually became CDC. His grasp of computer technology and the associated engineering concepts, coupled with his understanding of cryptanalysis, was invaluable in keeping the United States ahead of the field in this critical skill. Tordella was also a leader in securing American communications, pushing a series of leading-edge new encoding devices to secure U.S. government communications.

(U) During the Eisenhower administration, when the central concern of the government was the growing Soviet nuclear capability, Tordella led the NSA response. He was the driving force behind NSA's response to the threat, and he directed the technical activities of the Agency at a time when President Eisenhower had little else to rely on except signals intelligence. In 1958 Tordella convinced Eisenhower to fund a new communications initiative, called CRITICOMM, which offered a means to get critical intelligence information to the White House within ten minutes. The new system revolutionized concepts in American intelligence, bringing with it methodology that is still in use everywhere within the defense and intelligence communities.

(U) As a senior official at NSA, Dr. Tordella played a central role in NSA's outside relationships. Close collaborators in Great Britain and the British Commonwealth built up such a trust with Tordella that many foreign intelligence officials regarded him as the linchpin in their relationship with NSA. He traveled throughout the world building up that trust, and it paid great dividends over many years. He also served as the principal contact between NSA and its American collaborators: CIA, DIA, and the Office of the Secretary of Defense.

(U) In July of 1958, while he was serving in a liaison post to the Secretary of Defense, Tordella was asked by then-Director Lieutenant General John A. Samford to become his deputy. Tordella took office on 1 August 1958, and he continued as the deputy to six successive directors until his retirement on 21 April 1974. He thus became the longest-serving high intelligence official since World War II. Within

(b)(3)-P.L. 86-36

9/23/2010

NSA, he became an institution, and to many he WAS NSA. There was not then, and never has been since, a precedent for his tenure.

(U) Dr. Tordella received unprecedented honors over the years. On his retirement in 1974, the Secretary of Defense, James R. Schlesinger, presented him the National Security Medal. That same month he received the National Intelligence Distinguished Service Medal from the Director of Central Intelligence, William Colby. His relationship with the British was officially recognized in 1976 when he become an Honorary Knight Commander of the Most Excellent Order of the British Empire. After his retirement, he remained active in the intelligence community, serving on a number of boards and committees and as a consultant to various corporations with national defense contracts. In 1992 the Security Affairs Support Association, comprising mainly retired intelligence officials, gave him the William O. Baker Medal for distinguished service to American intelligence.

****

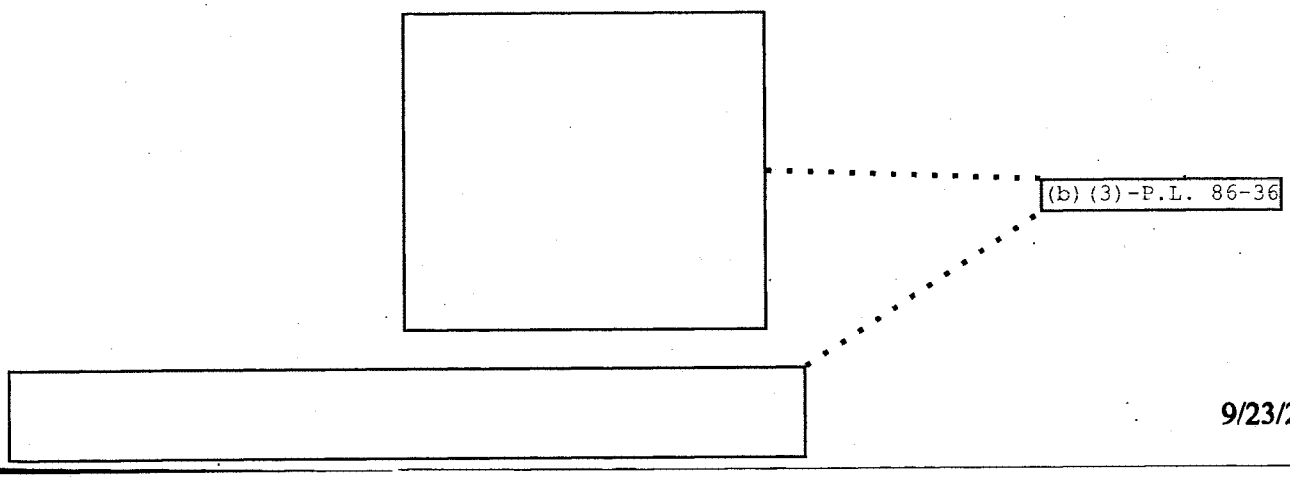
c. (U) C M I M A T H F E S T '9 6

(U) The CryptoMathematics Institute is pleased to announce the second annual MATHFEST, a daylong festival on Thursday, May 30, 1996, at the R&E Symposium Center. To cap off the festivities, the CMI banquet will be held in the evening at CoCo LoCo in Washington, D. C.

~~(FOUO)~~ The goal of MATHFEST is to bring together the entire NSA cryptomathematics community, if only for a day, to expose the variety of ways mathematics has recently contributed to the success of NSA's mission and to highlight the immediate challenges facing us. To accomplish this goal, the MATHFEST program will consist of a series of fifteen-minute briefings, each highlighting accomplishments of, or challenges to, an individual Office, Division or Branch. As the organizing committee envisions the event, each talk will be given by an analyst, at a level accessible to the entire CMI membership, and will give an overview rather than technical details. Of course, to accommodate all of our members, the talks must be suitable for CCR/CCS contractors and all green and gold badge personnel.

~~(FOUO)~~ The organizing committee encourages submission of abstracts for MATHFEST talks to the Office representatives listed below. A member of a listed Office who wishes to submit an abstract should contact the corresponding representative for instructions. Individuals from outside these Offices are strongly encouraged to submit abstracts, too, but should contact the organizing committee directly. The deadline for the Office level talk nominations is March 1, and the organizers will announce the talk selections by mid-March.

OFFICE REPRESENTATIVES



~~(FOUO)~~ The CMI eagerly anticipates your participation in this exciting event. We welcome your comments and questions and ask that they be directed to a member of the organizing committee.

CMI MATHFEST '96 Organizing Committee:

[redacted] (b)(3)-P.L. 86-36

d. (U) Mathematics Education Partnership Program - Training Sessions for Speakers

~~(FOUO)~~ The Math Speakers Bureau (MSB) is an outreach program that allows NSA employees to give talks at local area schools. We are always in need of new volunteers to fill the numerous request forms that we receive each year. If you are interested in becoming involved in the MSB, contact the MSB Coordinator, [redacted]

~~(FOUO)~~ The Mathematics Education Partnership Program (MEPP) will hold training sessions for all volunteers interested in the Math Speakers Bureau. The first training session will be on 22 February at 1000. The talk that will be presented is the "Goldbug". The session will take place in the D5 Conference Room - 2B5038. If you plan to attend this training session, please contact [redacted] via e-mail [redacted] or by phone [redacted]

(U) We hope to see you there! (b)(3)-P.L. 86-36

6. (U) ACTION LINE

(U) QUESTION: "Does the CA Tech Track Review Panel use a blind review process when evaluating a candidate for the titles of Senior Member and Master? If it does not, please explain why."

(U) ANSWER: Provided by [redacted] Chairman of the CA TTRP

(U) If, when you say "blind", you mean that the evaluation process does not include the name of the individual being evaluated, then the answer is no. The process for Tech Track titles for the CA Tech Track Review Panel (TTRP) does include the name of the applicant. (And, the process is the same, for every level, not just Senior and Master.)

(U) The applicant is judged in nine categories. Some of these categories - Advanced Educational Training, Technical Publications, and External Recognition - could be done in this "blind" manner. For example, we could read the technical papers and evaluate this category without knowing the name of the individual.

(U) However, one category that every applicant must have is Specific Technical Accomplishments. This Tech Track evaluation is done by your technical peers, and the normal paper trail will not be sufficient.

[redacted] (b)(3)-P.L. 86-36

We encourage applicants to provide detailed examples for their technical work, in any format. ("What do you mean provide more technical details? - I am too busy doing great technical work to spend time jumping through another hoop - If I wanted to do that much writing I would go into management!") Thus, we spend a lot of our time going to the technical work force and asking about the quality of the technical work under review. We may ask the applicant to expand on specific areas.

(U) Another important category is Technical Leadership. Here again the paper trail is often not sufficient to separate fact from fiction. Again we go to the work force and ask questions. I have been impressed with how uniform the answers on a particular applicant have been. The technical work force knows who does good technical work.

(U) We recognize that since the name of the applicant is known, there is a danger of personal prejudice becoming part of the process. We attempt to overcome this by having a broad range of people on our TTRP. We also attempt to interview several sources for each applicant. The applicant is encouraged to bring information in any form to the panel. The applicant should be aware of all the appeal processes, if there is a concern that personal prejudice has entered into the process.

(U) In short, I do not believe that a good technical evaluation could be done in CA without so much detailed information that the identity of the individual would be known to the Panel. One of our strengths is that we are a community. When the Panel makes decisions, we try to make them as a community decision. Most of our feedback has indicated that the CA community is satisfied with the present process. Please feel free to contact me at any time with suggestions on how we can improve our process in general or address any personal concerns.

****
//////////

7. (U) PUZZLES AND PROBLEMS

a. Solution from December Issue (b)(3)-P.L. 86-36

~~(FOUO)~~ Only [redacted] successfully solved the December Puzzle!

(U) Remember, the words were already ordered. The list was originally 40 long, but the escape from the Nile of a rat has reduced it to 38 (read down the columns). The challenge was to identify the themes within the list, and recreate the original.

(U) The original list consisted of 40 phrases, sorted by the first word. The phrases fall into 8 categories, for seven of which you are given the second word. For the eighth you are given the first word. The words in the 7 categories are

1. as, be, he, ho, in - chemical symbols
2. au, o, oh, owe - all pronounced "o"
3. cardinal chicken cuckoo kiwi robin - birds
4. cheshire cleveland norfolk suffolk yorkshire - English counties
5. hear see taste touch - 5 senses
6. hen london military miracle oxford - Haydn symphonies
7. kentucky louisiana missouri rhode island tennessee - US States

For the eighth category, the answers are also birds

(b)(3)-P.L. 86-36

[redacted]

8. vulture eagle duck turkey magpie.

Categories 2 and 5 have one word missing. It should be an easy step to recover eau de Nil and smell a rat respectively.

****

b. Puzzle Challenge Extended

(U) We will hold over the KRYPTOS Kristmas Kwiz for one more month to give people a chance to earn that ice cream sundae. Remember, the highest score wins, so give it a try.

****

c. (U) Puzzles Wanted

~~(FOUO)~~ Our Puzzle editor would be delighted to receive some puzzles and problems for future issues, so please keep him in mind!

****
//////////
##########

(U) EDITORIAL CORNER

REMINDER: Submissions for the March issue are due by February 26th.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

(b)(3)-P.L. 86-36

\\\\\\\\\\

Return to Kryptos Home Page

NSA Home Page

[redacted]

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

CONFIDENTIAL

(b)(3)-P.L. 86-36

~~TOP SECRET//COMINT~~

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:20
(U)PE EXTERNAL PAGE

THE CLASSIFICATION OF THIS NEWSLETTER IS ~~TOP SECRET UMBRA~~

****
* TALES OF THE KRYPT *
****
March 1996

//
****

~~(TSC)~~ TABLE OF CONTENTS:

1. (U) CA Perspective
2. (U) Calendar of Events
3. ~~(TSC)~~ KRYPTOS News
4. ~~(TSC)~~ Word from the CACP
5. (U) Community Service
6. (U) Technical Health
7. (U) Problems and Puzzles

//

1. (S) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature [redacted] of IDA/CCS.

(b)(3)-P.L. 86-36

Some Non-traditional Opportunities for Cryptanalysts in the SIGINT Cycle (~~TSC~~)

(~~TSC~~) BIOGRAPHICAL INTRODUCTION. Let me start by pointing out that I differ from other essayists of this column in that I have been in this field only eight years, and at that I am somewhat of an outsider. My training is in mathematics, but I spent my previous life as a computational physicist. I was an outsider there too, in a different way, working with 'real' physicists to define and analyze experiments. I did learn that to do my work well, I had to learn the entire cycle of laboratory work: experiment, analyze, (re-)form questions, and return to experiment. (As a aside, this work in physics, involving analysis of very large data sets, turned out to be the best possible preparation for my subsequent Agency work.)

(~~TSC~~) Since I came to IDA/CCS eight years ago I have been exceedingly lucky to have worked on a number of interesting projects, all in the field of what has become known as [redacted] Thus my view of SIGINT is narrower than even my few years of experience might suggest, having been confined to working only one signal type.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(S) THE SIGINT CYCLE. Within this limited perspective, I have formed my picture of the SIGINT cycle. My version consists of a sequence starting (somewhat arbitrarily) with signal development, signal collection, diagnosis/exploitation of cipher into plain text, and analysis by linguists into intelligence reports. What is interesting is the interplay of the parts of the cycle. (For example, intelligence production may lead to further signal development, and so on.)

(~~TSC~~) The cryptanalyst (CA) participates primarily in the middle of the cycle that I have described (somewhat arbitrarily) as beginning with signal development. However, in order to have the greatest impact, the CA has to see the whole picture. I want to describe here some observations based on personal experiences as a (neophyte) CA in the other parts of the SIGINT cycle. Most CA's already delve into these "non-traditional" roles, so I am not saying anything new here. The only possible novelty might be in emphasis.

(S) SIGNAL DEVELOPMENT. I have been intrigued with the question "Why am I looking at these particular bits from this particular signal?" Someone, somewhere has (1) decided that a particular communication contains interesting information, (2) identified and collected the signal, (3) demodulated (and possibly modified and filtered) the data, and (4) produced the cipher I finally see.

(S) In each of these steps
choices have been made, which we as CA's can and often should affect. For example, as CA's, we may have developed plain text or traffic analysis that could bear on signal ID and importance, especially if we are the first to see the decrypt. On the other hand, how often have we heard of crucial parts of the data having been thrown away because people did not understand their cryptographic significance (cf. part (3) above)?

[redacted]

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted] (b)(3)-P.L. 86-36 9/23/2010

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(S) In a growing number of further instances, CA's are contributing to the solution of problems previously thought to be intrinsically from the distant world of signals analysis. A recent example is the [redacted] workshop, which greatly benefited by the participation of CA's and statisticians. It was a goal of the workshop to include CA's, to benefit from their expertise, and it worked.

(S) Conversely, it was in the course of [redacted] problem that it became crucial for our diagnostic work to better understand the nature of the original collection. This led to one of the most productive collaborations I have had at the Agency, one between our small group of CA's and [redacted] His explanation of the collection environment, the natures of the types of interferences, was a revelation to us. And we, in turn, educated him on our collection requirements, all to the benefit of our project.

(FOUO) INTELLIGENCE ANALYSIS. Some of the most interesting Agency groups I have had the fortune to work with are the linguists and intelligence analysts. These are often very learned and cultured people, from a milieu completely different from my everyday world.

(FOUO) In my view we, as CA's, must do everything possible to make their work as easy and productive as possible. This means talking to them and trying to understand their world. They often protest against change, wanting to stick with what they are used to, which is understandable since they often work under pressure. However, if we learn the circumstances of their work, we can contribute new information sources and methods of presentation which will benefit us all.

(FOUO) I have left out discussions of a number of non-standard areas (reverse engineering, for example) which CA's can both contribute to and learn from. Let me finish by observing how far the search for the information I needed in order to do my job has led me from my original mathematics training.

---

2. CALENDAR (U)

Mar 4	Seminar on Certification (9A135, 1000-1130)
Mar 14	KRYPTOS Talk, [redacted] on "Classical Cryptanalysis - The Folger Manuscript", (Friedman, 1300)
Mar 14	Science & Engineering Society Presentation (S&ES) - "MISSI - The Multilevel Information System Security Initiative", [redacted] (1000 R&E Symposium Center)
Mar 18	KRYPTOS Talk - [redacted] GCHQ, "Reminiscences from Bletchley Park", (ZB4118, Rm 6) SEATING IS LIMITED. Preference will be given to KRYPTOS members until 0855.
Mar 25-29	CARD, at CCS

(b)(3)-P.L. 86-36

PLAN AHEAD

Apr 10	S&ES Sixth Annual Luncheon, (Canine Suite, 1100)
Apr 25	"GNI - The Attack has Begun", (Friedman 0800-1600)
May 13-17	ACE 1996 at CCS in Bowie.
May 21-22	CA PQE
May 28	CA-305 Begins
May 30	MATHFEST '96 and CMI Banquet
June 18	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)
Sep 17	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)
Fall?	CONSCRYPT '96, at DSD
Nov 19	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)

---

3. (FOUO) KRYPTOS NEWS

a. (U) Special KRYPTOS Speaker Announced

(S-CCO) [redacted] has kindly volunteered to present a KRYPTOS talk while he is in the US in mid-March. He will talk about some of the excellent work done at Bletchley Park durings its colorful history,

[redacted]

including their exploitation of TUNNY and the COLOSSUS attack on it. Only 60 seats are available in this conference room. KRYPTOS members only will be seated until 0855, when, if seats are still available, non-members may be seated.

---

b. (FOUO) Membership Drive Gets "Mugged"

(U) The following people won KRYPTOS mugs in the 1996 KRYPTOS Membership Drive. Many thanks to all who have joined KRYPTOS this year: as of today, we have a total of 215 members, of which 103 are new members in 1996.

(FOUO) Winners should contact [redacted] preferably via email [redacted], and state whether they would like a mug or the alternate prize of a KRYPTOS pin. We will then arrange for delivery of the prizes.

(U) We are still accepting memberships for 1996, both new and renewal.

(FOUO) And the winners are:

[redacted]

(b)(3)-P.L. 86-36

---

c. (U) Joint KRYPTOS/CMI Festivities a Success

(FOUO) [redacted] organized this year's gathering and reports that on Tuesday evening, February 20th, 55 Kryptos and CMI members converged on the Last Chance Saloon in Columbia for a 'Fat Tuesday' social gathering. The Last Chance provided us with their back room, and twice brought out an impressive array of appetizers. There was very little left on the serving table afterwards, although the 29 kegs of draught beer offered that night were in no danger of suffering a similar fate!

//

4. (U) Word from the CACP

a. (U) REVISION TO COMPUTER PROGRAM REQUIREMENT

(FOUO) The CA Career Panel is in the process of revising its criteria for professionalization, and has just completed a new document describing the computer program requirement for certification. If you would like a hard or soft copy of this revised document, please call or email [redacted] or stop by the CA Career Panel office in OPS 2B room 3036D.

(b)(3)-P.L. 86-36

[redacted]

b. (U) CA-305, Cryptanalysis: Contemporary Issues, Announcement

(U) The annual offering of CA-305 will be held May 28 - June 5. This annual symposium will take place in Friedman Auditorium and several Ft. Meade conference rooms.

(FOUO) The symposium is designed to bring cryptanalysts, crypto-mathematicians, computer scientists, engineers, signals analysts and other interested persons up to date on the status and trends in the current practice of cryptanalysis. The symposium will be presented as a number of individual lectures by competent authorities on a variety of cryptanalytic and related subjects with questions and discussions by the participating students.

(FOUO) If you would like to present a 30 - 60 minute talk on any cryptanalytic topic for the 1996 symposium then you must:

1. Obtain your management's approval to present the talk.
2. Submit an abstract for any cryptanalytic or cryptanalytic-related presentation to the Z/CAO for review accompanied by a conference approval sheet signed at the Branch level. The Z/CAO must verify that the topic(s) are releaseable to all conference participants. The current Z/CAO is [redacted]

   Procedures for approval of CA or CA-related topics and the approval sheets may be obtained from [redacted] or downloaded from the internal Z Homepage on MOSAIC.
3. After the talk abstract has been approved please send both abstract and approval sheet to the 1996 CA-305 course coordinator [redacted] or via e-mail to [redacted]

(FOUO) Suggestions, comments, or questions can be submitted to [redacted] at the above addresses or via phone at [redacted] The deadline for submitting talks for this year's CA-305 is TUESDAY APRIL 2, 1996.

(b)(3)-P.L. 86-36

---

5. (U) COMMUNITY SERVICE

a. (FOUO) Science and Engineering Society Presentation Announced

(FOUO) The Department of Defense is at a crossroads with respect to security for its networked information system architecture, which consists of many individual systems based on open system concepts using best available commercial technology. Significant portions of this architecture are composed of unsecure commercial networks like the INTERNET. [redacted] will address the philosophy and programs for providing the necessary connectivity between systems of all classification levels, while protecting all systems from unauthorized access and assuring their availability at a reasonable risk.

(FOUO) [redacted]

(b)(3)-P.L. 86-36
(b)(6)

(FOUO) This presentation will be broadcast on Newsmagazine Channel 17.

---

b. (U) Center for Cryptologic History (CCH) Announcement

(U) The NSA/CSS Archives will soon release approximately 1.55 million pages of declassified historic material to the National Archives and Records Administration (NARA). These documents include such items as correspondence between foreign governments relating to diplomatic, commercial and military intelligence during both world wars, including: Mexican codes and ciphers from 1912-1918, cipher bureau operations from various countries from 1914-1918, German post-World War I historical analysis and naval operations from 1912-1935, the Pearl Harbor investigation, interrogations of Russian Prisoners of War by their German captors, intelligence activities in the Philippines from 1934-1941, use of Native Americans as communicators, the war diary of the German "U427" submarine, and documents concerning German cessation of hostilities at the end of World War II.

---

6. TECHNICAL HEALTH

a. (FOUO) Public Key Cryptography Seminar Announced

(FOUO) There will be a seminar on the fundamentals of public key cryptography on 14 March, 0900-1100, in 9A135. This seminar, which is the first of a series of Public Key presentations, will be open to everyone in Z. [redacted] is the POC.

(b)(3)-P.L. 86-36

---

b. (U) Seminar on Certification

(U) The execs of the Math, CA, and CS career panels will conduct a seminar on certification on Monday, 4 March 1996, from 1000 to 1130

[redacted]

hours in room 9A135 of the Headquarters building. The presentation is designed for mathematicians, but any NSA employee interested in knowing about professionalization in these career fields is welcome to attend. After describing the requirements and process for their career fields, the execs will answer questions from the floor.

---

7. (U) PUZZLES and PROBLEMS

(FOUO) Solutions from the GCHQ Kryptos Kristmas Kwiz were received by

[redacted] (b)(3)-P.L. 86-36

The answers are as follows:

ANSWERS

2. (a) SPADING - 2 (b) RELOCATING - 4 (c) ABRACADABRA - 69

3. (a) al/b/bl/br/f/fl/fre/fr/he/kn/l-ight
(b) b/d/p or n/pr/qu/t/w-icker
(c) dawn/dot/grant/mark/matt/nick/pip/rob/will-ing

4. All were named after the people who were associated with their introduction.

5. Kim and Pak, the two most common family names.

6. All were written, in part or in whole, in prison.

7. All were born of unmarried parents.

8. (i) GEMINI (ii) 12 (iii) LAIKA

9.

CONDITION	CONFEDERATED	CONSONANT	IMPORTANT	ORTHOGRAPHER
PARSONAGE	PERSONAGE	REPORTAGE	REPORTERS	

10. Between box and bat.
There are five sets of ten words: the words are sorted according to a word associated with each of the listed words. The five sets are words:
(a) that can be preceded by a Greek letter to form another word;
(b) that are associated with three-letter words ending in X;
(c) follow various sports;
(d) which form a phrase of the form "xxxx the xxxxx"
and (e) which form the title of a Sherlock Holmes adventure.
and (e) which form the title of a Sherlock Holmes adventure.

alpha/bet	beta/max	bowling/alley	box/clever
boxing/ring	cardboard/box	cricket/bat	croquet/lawn
dancing/men	delta/wing	empty/house	engineer's/thumb
final/problem	fox/brer	gamma/dion	golf/club
Henry/eighth	hockey/stick	illustrious/client	kick/bucket
lily/pink	max/factor	mu/slim	nobel/bachelor
Norwood/builder	nu/clear	over/moon	phi/lately
pi/lot	pop/question	pox/chicken	pull/plug
red/circle	rex/tyrannosaurus	rock/boat	rugby/union
Rupert/bear	sax/tenor	sex/gentle	pack/six
snooker/table	solitary/cyclist	squash/court	swimming/pool
take/biscuit	tau/rus	tax/income	vox/pop
winnie/pooh	CHI/CANE		

11. Driving Miss Daisy (motion Picture Academy Awards, Best Film 1989)

12. (a) 13 [x(t)=x(t-1)+x(t-2)] (b) 29 [x**2 - 3x + 1]
(c) 1844 [3**x - x**3] (d) 4697 [x! - x**3]
(e) 1909 [4**(x-1)-3**x]

13. The text conceals 10 US states (Missouri, Idaho, Utah, Texas, Ohio, Washington, Georgia, Kentucky, Indiana and Oregon).

14. (a) STEPHEN and JOHN (b) YCGGCKL AND NOIE

(c)

K	I	N	G	S	A	N	D	Q	U	E	E	N	S
7	6	8	5	12	1	9	2	11	14	3	4	10	13

M	O	N	A	R	C	H	Y	B	D	E	F	G	I
J	K	L	P	Q	S	T	U	V	W	X	Z		

The list gives the kings and queens of England, enciphered using the alphabet CSYUEXFZAPOKMJNLHTGBVRQIDW. The slide is given by the number following the monarch's name: there was only one Stephen and one John, so no number follows their names. James II was followed by William (III) and Mary (II).

15. Letters in the first set:
(a) are symmetrical about the vertical
(b) have Morse Code equivalents beginning with dot
(c) appear in "KRYPTOS KRISTMAS KWIZ"
(d) appear in the Russian alphabet
(e) have a hole in the first position of the second row in Braille

16. HAVE RECRUITED TOP G.C.H.Q. CRYPPIE. THE FERRET.

The key comes from 5-figure trigonometrical tables - starting

[redacted] (b)(3)-P.L. 86-36

with sine (S) 15 degrees:

Key: 25882 27564 29237 30902 32557 34202 ...
Plain: 04343 80944 16091 51637 06450 94644 ...

Cipher: 21549 47620 13246 89375 36107 40668 ...

17. Ngwee (the currency in Zambia) or tambala (ditto Malawi).

18. EIRE, SYRIA, ZIMBABWE, ZAMBIA.
-N delete the letter at position N
+N insert A at position N
(M,N) exchange the letters at positions M and N
N+/N- replace the letter at position N by the letter which follows/precedes it in the normal alphabet

19. SOME (awe fear hand lone tire win whole-some;
some- body day how one thing what where)

20. REST 1a (The)re's t(ranquility) 5a (S)ever(n)
EVER 6a (A)dele 7a (comm)only
DELE 1d Oder reversed 2d even(t)
ONLY 3d sell = Scots self 4d t(h)r(e)e(b)y

21.
1 (Man and His Dog) 4 (Farthings in an Old Penny)
2 (Shakes of a Lamb's Tail) 8 (Pints in a Gallon)
5 (Days in a Working Week) 7 (Wonders of the World)
.142857 recurring = one seventh

22. (a) They are all the same person
(b) Rebecca West
(c) All (year of birth)

23. Zaire

24. Sweden (Hungary, Albania, Luxembourg, Lichtenstein, Austria, Norway, Denmark lead to HALLAND)

25. (i) SLOSH. The 15 words are LOO (100), LEE (144), LAP (169), GAL (361), EEL (441), ASH (625), PAL (961), LOSE (1024), SHOO (2500), STOP (2809), GOSH (3025), EASE (4624), HASH (5625), CHAP (7569) and POSH (9025). SLOSH is 21025 (145**2).

(ii) ERROR. The words are RE (64), AGO (125), GAR (216), ABBA (1331), GAMS (2197), AIRED (10648), AGARS (12167), and BOMBS (35937). ERROR is 46656 (36**3).

26. BEETHOVEN. (BRAHMS, BRUCKNER, SCHUBERT, TCHAIKOVSKY, MAHLER, MOZART, DVORAK, SIBELIUS, MENDELSSOHN)

27. (a) 121 N**2 base 9
(b) 6 diagonal pattern on keyboard
(c) A9/109 N**2 base 16
(d) M N**3 mod 26
(e) 841 sum of proper factors of previous value
(f) 18 N(I)=N(I-1)+12
(g) 107 N(I)=N(I-1)+ sum of digits
(h) 4506 N(I)=N(I+1)+ product of digits
(i) 44 N(I)=N(I-1) + difference between digits
(k) 14641 N**4 base (N-1)
(l) Q alternating letters of "to be or not to be..."

28. Rule 1: N=2 (number of symbols in Morse Code equivalents)
Rule 2: N=8 (length of Nato phonetic equivalents)

29. (a) PIZZAZZ (b) UNOSTENTATIOUSNESS (c) GYMKHANA, SYZYGY

30.
```
Q U I Z   A X   C   E D G E
A   M H O S   J O W L     V     (3 x 14 = 42 squares)
T Y P O   K N O B   F I R E
```

31. 903422 (ZODIAC). Substitution is

0	2	3	4	5	6	7	8	9
O	A	D	G	J	M	R	U	X
Q	B	E	H	K	N	S	V	Y
	C	F	I	L	P	T	W	Z

(based on the old telephone dial)

32. LADIES and GENTLEMEN in Welsh.

33. (a) OOOXX reject all hearts and spades greater than 7
(b) OOXOX reject 1 card after a black face card; reject 2 after a red non-face card; reject 3 after a black non-face card
(c) XOXXO only red after even, only black after odd

34.
1. William Wallace
2. Arthur Hallam
3. Roy Orbison
4. Richard Rogers
5. Edward Lear
6. Laurence Olivier
7. Lech Walesa (1983: note initials)

---

b. (U) NEW PUZZLES

(U) The following are puzzles that I pulled (with the author's permission) off the outside web. If you have outside internet access,

(b)(3)-P.L. 86-36

you may want to visit the author's site at:

http://www.webcom.com/~clong/welcome.html

You are on your honor to submit your own solutions, and not those you found on the web! Submit answers to either or both puzzles.

Puzzle #1: Birthday Ununiqueness (U)

I was sitting around with my friend Waldo and his grandfather Mortimer last week, and the topic of birthday surprises came up. Mortimer mentioned that one of the greatest surprises that he has had involved his grandfather, who happens to have the same birthday that Mortimer has. One year the family was celebrating this double birthday, and during the events Mortimer proudly mentioned to his grandfather that not only had he just turned as old as the last two digits of the year he was born in, but he was also a prime number of years old, and each of the two digits making up his age was also a prime. Mortimer was floored when the older man thought for a second, turned to him, and said that the same thing had just happened to him! What year did this occur, and how old had Mortimer and his grandfather just turned?

Puzzle #2: Fast Answer(U)

I was sitting around with my friend Waldo, his nephew Spike, and Spike's friend Molly recently. I happened to have two tickets to a new movie in my pocket that I had just purchased, and I mentioned this and noted that there were two four-digit numbers on the tickets and that the sum of all 8 digits was 25. Waldo asked if any digit appeared more than twice out of the 8, which I answered. Spike then asked if the sum of the digits of either ticket was equal to 13, which I answered also. Much to my surprise, Molly immediately told me what the two numbers were. What were they?

//

##

(U) EDITORIAL CORNER

REMINDER: Submissions for the April issue are due by March 27th.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

(FOUO) EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted] (b)(3)-P.L. 86-36

[redacted]

\\\

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2, DATED 3 SEP 1981
DECLASSIFY ON: SOURCE MARKED "OADR" DATE OF SOURCE: 3 SEP 1981

[redacted]

TOP SECRET//COMINT

~~(S)~~ POC: [redacted] info
(U) *Last Modified: 10/30/2002 11:42:19*
(U)PE EXTERNAL PAGE

THE CLASSIFICATION OF THIS NEWSLETTER IS ~~TOP SECRET UMBRA~~

(b) (3)-P.L. 86-36

```
**********************************
*        TALES OF THE KRYPT      *
*                                *
*        APRIL 1996 ISSUE        *
**********************************
```

//
****

~~(FOUO)~~ TABLE OF CONTENTS:

1. (U) CA Perspective

2. (U) Calendar of Events

3. ~~(FOUO)~~ Word from the CACP

4. (U) Technical Health

5. (U) Community Service

6. (U) Problems and Puzzles

//

1. (U) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month, however, we are pleased to feature Phorme Z. O'Fisceef, now retired from the fifth office, reporting on the latest happening in the CA Community.

MATHEMATICS BANNED IN Z GROUP

(U) FORT MEADE, MD, 1 April 1996, - At an off-site attended by Z Group Office level management held last week, a decision was reached to ban the use of mathematics in Z Group. This decision was announced by the Chief of Z to a packed audience of Z Group employees in the Friedman auditorium this morning. The chief said, "We have the blessing of the Director to implement this plan as a major budget-saving initiative." He further quoted the Director as saying "...it could be a model for the rest of the Agency and the Federal government {the Agriculture Department has been using this approach for years}. We are looking at language analysis, computer science and engineering to see if a similar plan might work in those disciplines." After announcing that the decision was based on the enormous savings that could be made, the floor was opened to questions from the audience addressed to the Z managers on the stage. What follows is a sampling of the questions and answers and some observations made by individuals in Z Group who have provided their thoughts on condition of anonymity.

(U) A thoughtful questioner wanted to know what would happen to the data that Z normally processes. One of the Office Chiefs, after a considerable pause, gave a lengthy and complex answer. The consensus of those

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

who heard the reply boiled it down to the following: "We will aggregate the letters into separate bins without counting them or detailing their position.". There was a follow-up question: "What about binary data?" "That's an easy one.", another Office Chief answered to a collective sigh of relief from the audience. "Just aggregate the 1's and 0's.". "Can you count them?" rejoined the canny questioner. "No, that would be too mathematical.", came the reply. A squeaky voice in the back of the auditorium asked about data that was not character- or bit-oriented. An Office Chief responded that "...it would be unnecessary to do any analysis or measurement on such data and therefore the operation of my office will not be affected by this decision.". The next question had to do with computers and their use in Z. "No problem." stated an Office Chief acridly. "Also there will be no change in the plan to put a CRAY YMP on every analyst's desk. With that type of computer power, who would need to do mathematics anyway?"

(U) In a related development, it was reported that MITAGS held an emergency meeting on the decision. They reached a major conclusion that it would be necessary to convene an off-site, but the meeting ended in confusion as the attendees got bogged down over whether the off-site should be held in Charlottesville or Berkeley Springs! Also, a senior technical level individual was heard to mutter under his breath, that this was merely another grandstanding display by the math community to force the cryptanalysts out of the limelight.

(U) Continuing with the questions from the audience to Z Management, a most logical and practical question was asked: "What will happen if someone actually does Mathematics in Z Group?". The Staff Chief promptly replied: "The first offense will be an assignment to Z5. If you are already in Z5, that will be punishment enough. A second offense will land you in R5 or C6. For a third offense", she replied with a twinkle, "the miscreant will be sent directly to La Jolla without passing through Princeton or receiving a relocation bonus". The next quesion was "What would happen to the Cryptomathematics Program?" An Office Chief replied, "Nothing.", and sat down. The Chief of Z hastily amplified on this answer: "Their tours would be the same, they just would not do any Mathematics." A follow-up question was "What about the math hiring program?" The Chief of Z, visibly rankled by this obtuse question replied: "It is obvious that the hiring program for mathematicians must continue. How else will we be able to achieve substantial savings in the future?" At this point, our anonymous observer reports that it was as if the entire management team on the stage smiled as one, and appeared to be puffed up with their own importance and brilliance. In reality, though, and they all stood up and shouted in unison "April Fools".

~~~~~~

****

//////////

2. CALENDAR (U)

Apr 3	KRYPTOKNIGHTS Roundtable, Camelot, England
Apr 10	Lambros Callimahos Birthday Celebration, Athena Restaurant, Pigs Brains Special
Apr 25	CA-400 Class 2000 Reunion, Hausner's Carry-Out

PLAN AHEAD (U)

(b)(3)-P.L. 86-36
~~~~~~

May 13-17	ACEventura Conference on the PET Random Number Generator, David Bowie Center
June 17-21	Zendian Cryptodevices Exhibit, National Cryptologic Museum
Sept 11	KRYPTOS Talk, Bawlmor Sun Expert on Cryptology (Friedman Auditorium, 1300)

****
//////////

3. (U) WORD FROM THE CACP

(U) Call for Committee Volunteers

(U) The CACP announces a call for volunteers to serve on a committee to assess the role of psychic CA in breaking cryptologics. This is a follow-on effort to last year's highly successful development of telepathic algorithms for depth reading. Interested analysts should apply to R. U. Serious at 913-1313s or by e-mail to Sy Kick @frnds.netwrk.

****
//////////

4. (U) TECHNICAL HEALTH

TECH-TRACK QUALIFICATION EXAM (TTQE)

By Mike Kelly, former Z43 SLE, now retired

(U) Through extensive research by members of the Technical Track Board, it has been determined that to select for Tech-Track membership from among the many otherwise qualified technical personnel in this organization, a method of determining their abilities in related fields must be established. Subsequently, we have contracted the National Union of Testing Systems (NUTS) to provide a related-fields testing program for Tech-Track applicants.

(U) A score of 95 or better is required of each successful candidate. Answer all questions thoroughly. You will be given three hours.

(U) 1. ECONOMICS - Develop a realistic plan for retiring the national debt. Include provisions for the possible effects of your plan on the wave theory of light and on the overcrowding of Citizens' Band radio channels.

(U) 2. ENGINEERING - The disassembled parts of a high-powered rifle will be placed on your desk along with an instructions manual printed in Swahili. In ten minutes a hungry Bengal tiger will be admitted to the room. Take whatever action you feel appropriate. Be prepared to defend your decision.

(U) 3. MEDICINE - You will be provided with a razor blade, a piece of gauze and a half-bottle of scotch. Remove your own appendix. Do not close the incision until you work has been inspected.

(U) 4. PHILOSOPHY - Sketch the development of human thought, and describe

(b)(3)-P.L. 86-36

its significance. Compare and contrast this with other kinds of thought.

(U) 5. PHYSICS - Explain the nature of matter. Include in your answer an evaluation of the possible effects of electromagnetic emanations from commercial power lines on the reproductive health of Giant Pandas.

(U) 6. POLITICAL SCIENCE - Pick up the gray phone and start World War III. Report at length on its socio-political effects, if any.

(U) 7. PUBLIC SPEAKING - 150 riot-crazed members of an unidentified aboriginal tribe will be turned loose in the classroom. Calm them. You may use any ancient languge except Greek and Latin.

(U) 8. RELIGION - Trace the history of all religions from their earliest origins to the present day. Prove which is best in a manner which will convince all other religions.

(U) 9. SOCIOLOGY - Estimate the sociological problems which might accompany the end of the world. Contrive and conduct an experiment to test your hypothesis.

(U) 10. UNIVERSAL KNOWLEDGE - Describe everything you know in detail. Be objective and specific.

(U) 11. EXTRA CREDIT - Define the Universe; give three examples.

****
//////////

5. COMMUNITY SERVICE (b)(3)-P.L. 86-36

a. SECOND PARTY CA TRAINING: MONGOLIA ~~(TSC)~~ By [redacted]

~~(TSC)~~ One of the most interesting three weeks of my NSA career has been my recent Mongolian TDY to teach introductory CA courses. Despite the untimely loss of the presumably late [redacted] the trip was an unqualified success, improving the relationship between NSA and an important Second Party partner.

~~(TS-GCQ)~~ As you may know, GKHQ (Genghis Khan Headquarters) replaced GCHQ as a second party recently, due to "Mad Cryppie Syndrome" caused by the British beef offered at Wood dining facilities (one analyst, [redacted] was found riding the freight elevator for four days muttering about unsolved Austro-Hungarian ciphers he apparently worked as an intern. He was given a face-saving retirement last week). In exchange for the cafeteria receiving monthly shipments of Mongolian yak meat, NSA agreed to provide cryptanalytic expertise against [redacted] This resulted in my training TDY, accompanied by [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(S-GCQ)~~ GKHQ is a rather primitive facility, being a collection of five yurts located a mere 20-minute horse ride from booming downtown Ulan Bator. Perched on a high, treeless plain, there were no security fences, and a herd of oxen served as a classified waste disposal system (interns monitored the herds output in case of incomplete destruction). Except for the initial beating we received because they thought we were Russian, the Mongolians proved to be excellent hosts,

(b)(3)-P.L. 86-36

[redacted]

giving us unexpectedly full tours of all five yurts, including the director's, which had the nicest grass.

(TSC) The Mongolian students were hard workers, and were proud of their agency. They enthusiastically demonstrated their new CA LAN, which consisted of seven abacuses hooked to a large 10-by-20-foot abacus, with ceramic beads. "We can figure out problems on our local machine, or logon to the big mainframe for large number-crunching problems." A burly, unshaven man named Ugh operated the mainframe. Obviously highly paid, he offered to purchase [redacted] for a tempting price. Only when she promised to buy us dinner did [redacted] and I refuse.

(TSC) All went well until our farewell dinner, a splendid repast of broiled yak, basted marmot lungs, camel cheese and a myriad of undefined vegetables, served with an unchecked flow of Mongolian vodka. Despite our cryptanalytic background, we negotiated the social niceties flawlessly until [redacted] mentioned how proud he was to learn that the Washington Post had recently selected Genghis Khan as Man of the Millennium.

"I think that's a bit premature," [redacted] suggested, remarking that five years still remain until the millennium's 'technical' end on 31 December 2000, and that, besides, "Prince Henry the Navigator deserves the award."

(b)(3)-P.L. 86-36

(U) With that, the back flap of the yurt opened up, allowing two lightning-footed steeds carrying wild-eyed Huns to race through the tent and snatch [redacted] from his meal, spitting sheep eyes as he

(U) We were still chuckling about poor [redacted] at the airport the next morning, until the realization set in, along with our hangovers, that he was not going to make the flight. However, we still had a wonderful trip, and decided not to worry too much about [redacted], especially since the Mongolians had unexpectedly provided us with a crate of special meat to present to the cafeteria as a gift from their president. "It will taste like nothing you have ever had before," Mr. [redacted] said.

(U) As an epilogue, the meat was served last week as part of Wood Dining's Tour of Asia, and was a big hit, tasting vaguely like chicken in the Mongolian Barbeque.

---

b. Z PERSONNEL NEEDED FOR OLYMPIC WORK (TSC) By [redacted]

(TSC) In light of NSA being named the Official SIGINT Organization of the United States Olympic Team, cryptanalysts, cryptomathematicians, collection managers and computer scientists are being recruited throughout Z to participate in the Agency's Olympic Effort. According to [redacted] and Olympic Task Force Leader, this will be a golden opportunity for Agency employees to excel. "For years, we attacked the Soviet problem, but never actually had to fight a war against them, so our effort was wasted. But we KNOW we will have to oppose the Brazilian basketball team. For once, we can do something that matters."

(b)(3)-P.L. 86-36

(TSC) NSA won "Official" status in a tight competition with SIGINT organizations from Japan and Mexico, whose cheap labor and offer to take Texas back made it a favorite choice of President Clinton's campaign advisors ("Bill, we're not going to win those electoral votes

[redacted]

anyway," one was overheard saying.) In the end, however, it was Z's cryptanalytic capabilities and the anti-Castro lobby that made the difference: no one else would task as many collection resources against the Cuban third base coach.

(TSC) The biggest CA effort will obviously be in baseball, where Team Chief [redacted] expects to have five cryppies, two data flow and one system administrator working each game the US plays, and three CA personnel scouting future opponents. "We should be able to predict every bunt, steal, and split-finger fastball before it happens," [redacted] said, "this should make the game much easier on our players, who aren't that bright to begin with. Can you believe thay can't even solve a single transposition?"

(TSC) Another big push will be on the drug testing target, where [redacted] will lead a team of password guessers trying to break into the IOC's computers. "We can change the test results of all the Chinese swimmers to positive, really giving a boost to our women's team," [redacted] notes. "We can also find out what drugs are not being detected, and encourage our athletes to take them." Asked if he had any ethical problems with such endeavors, [redacted] replied, "Me?"

(TSC) Asked how much this would cost, budget analyst [redacted] said, "Tons, especially if you count the toilet I just busted." So what does NSA get in return? "Well, as official sponsors, we think that the intelligence community will be more interested in our product," a laid-back [redacted] opined, "and I'll get to ride in that cool NSA/Hertz-Rent-a-Car blimp."

(FOUO) For those interested in joining this task force, contact the following people:

Baseball
Basketball
Volleyball
Synchro. Swimming
Soccer
Boxing
Cycling
Wrestling
Gymnastics
Drugs

[redacted]

(b)(3)-P.L. 86-36

****
//////////

7. (U) PROBLEMS AND PUZZLES

a. CRYPTO-TALK (U)

(U) Brush up on your cryptanalytic terminology by finding 52 terms of modern cryptanalysis. The terms read in a direction. Score two points.

****
additiveaaaaaaaaaaNihilist
ADFGVXbbbbbbbbbbnonliteral
Baconiancipherconepartcode
BCDddddddddddddddddopencode
CAeeeeeeeeeeeeeeeeepadding

(b)(3)-P.L. 86-36

[redacted]

cryptanalysisffperiodicity
deciphermentgggggggqsignal
decodehhhhhhhhquantization
enciphermentiiradioprinter
encodejjjjjjjjjjjjjjjrotor
FibonaccikkkkkkkkkkkkkkkkkSCE
flatlllllllllllllllllSIGINT
garblemmmmmmmmmmmmmmmmmmmmmmmmmTA
Gronsfeldnnnteletypewriter
Hagelinooooooundulatortape
hitpppppppppppppuniliteral
ICqqqqqqqqqqqVernamaddition
intervalrrrrrrrrrrVigenere
jargonsssssssssssswhitebox
juniorwheelttttttttttttword
kappaplainuuuuuuuuuuuuuuuuuX
kapparandomvvvvvvvvvvvvvxiIC
LatinsquarewwwwwwwwwwwwwYOU
lowgradexxxYOUWENTTHISFAR?
masterdecoderyyyyyyyyZendia
messagezzzzzzzzzzzzzzzzzzZ0
****

"""""""

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

[redacted]

(b)(3)-P.L. 86-36

[redacted]

TOP SECRET//COMINT

~~(C)~~ *POC:* [redacted] *info*
(U) *Last Modified: 10/30/2002 11:42:19*
(U)PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
April 1996

//
****

~~(FOUO)~~ TABLE OF CONTENTS:

1. (U) CA Perspective

2. (U) Calendar of Events

3. ~~(FOUO)~~ Word from the CACP

4. (U) Community Service

5. (U) Technical Health

6. (U) Problems and Puzzles

//

1. ~~(C)~~ PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature [redacted] (formerly Chief, Z3) now a cryptanalyst working on [redacted]

(b)(3)-P.L. 86-36

~~(FOUO)~~ After spending about 10 years on a diversity tour in management, I have returned to the technical workplace to find some changes. Some are good, some are not. Some were to be expected, others were surprising.

~~(FOUO)~~ One of the first things to hit me is the increased capability and complexity of the computing environment. When I left, the CRAY-I was just coming in and I was amazed that a user could get hundreds of thousands of words of memory. There was no computer networking. There was no capability to plot waveforms or listen to a speech file on your own terminal. And, alas, there was no XBIT. One of the first things I did after getting access to a computer was compile a FORTRAN program with an array dimensioned to one billion words. The number of computers we have at our disposal and with the enormous storage capacity and compute power is staggering! (and I haven't yet used more than one processor at a time.)

~~(FOUO)~~ While the UNIX world is complex, my entry into it was easier than I expected. This was facilitated by a lot of help from our excellent core of system administrators and many friends who were very generous with their time and patience. I have been surprised at how dispersed the expertise is. You have to make a lot of phone calls to find someone who is knowledgeable about things I would think everyone would want to know. While I tried to spread the burden among a number of people (one doesn't want to appear too stupid) invariably some

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

people pulled double duty.

(FOUO) Another observation on the current situation is that there seem to be more distractions than before. I believe that crypt-analysis requires single-minded, deep focus. The large number of conferences, technical meetings, meeting meetings, technical talks, award ceremonies, town meetings, team meetings, TTRP meetings, ... makes that commitment more difficult than I remember it being.

(FOUO) The current problem set is certainly richer than I can ever remember. The problem I am currently working is so dynamic and exciting, I can't get enough time to do everything I should. In addition to that, I am aware of several problems in other areas that I would love to work on---if only there was time.

(S) The one area that really needs some improvement is our ability to store and quickly access large data files. While many people have been working on this, we still have great room for improvement. We have great difficulty dealing with 1970's technology (signals running

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(FOUO) While on my management tour, I had the perception that there was a disproportional amount of whining by the technical work force. I couldn't understand this because I believed that their work had a minimum number of negative aspects and a maximum of rewarding aspects. My recent change of jobs has only reinforced that view.

(FOUO) Great problems, great computer access, terrific people to work with-- What a great time to be alive!

****
//////////

2. CALENDAR (U)

Apr 3	Z Technical Health Awards Ceremony
Apr 10	S&ES Sixth Annual Luncheon, (Canine Suite, 1100)
Apr 25	"GNI - The Attack has Begun", (Friedman Auditorium, 0800-1600)

PLAN AHEAD (U)

May 13-17	ACE 1996 at CCS in Bowie, Maryland
May 21-22	CA PQE

(b)(3)-P.L. 86-36

[redacted]

May 28	CA-305 Begins
May 30	MATHFEST '96 and CMI Banquet
June 18	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman Auditorium, 1300)
June 18	Science & Engineering Society, June Symposium, (R&E, 1300)
Sep 17	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman Auditorium, 1300)
Fall?	CONSCRYPT '96, at DSD
Nov 19	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman Auditorium, 1300)

****
//////////
3. (~~FOUO~~) Word from the CACP

a. (~~FOUO~~) PQE Registration

(~~FOUO~~) Registration for the Professional Qualification Examination (PQE) is now in progress at the CACP office. Review sessions will be held during the month of April and the PQE will be given May 21 - 22.

****
b. (~~FOUO~~) CA-305, Cryptanalysis: Contemporary Issues, Announcement

(~~FOUO~~) The annual offering of CA-305 will be held May 28 - June 5. This annual symposium will take place in Friedman Auditorium and several Ft. Meade conference rooms.

(~~FOUO~~) The symposium is designed to bring cryptanalysts, crypto-mathematicians, computer scientists, engineers, signals analysts and other interested persons up to date on the status and trends in the current practice of cryptanalysis. The symposium will be presented as a number of individual lectures by competent authorities on a variety of cryptanalytic and related subjects with questions and discussions by the participating students.

****
//////////

4. (U) COMMUNITY SERVICE

a. (~~FOUO~~) Science & Engineering Society News

(~~FOUO~~) The sixth S&ES Luncheon will be held on Wednesday April 10, 1996 at 11 A.M. in the Canine suite. Our speaker this year will be Dr. Robert Hermann who will give us his "Thoughts on the Future of Intelligence"

(~~FOUO~~) Dr. Hermann will be remembered by some of us old timers as the "founder" of W group, a former DDR and Director of NRO. He is currently a member of the President's Foreign Intelligence Advisory Board(PFIAB), the DOD Science Board and the Aspin/Brown commission.

(b)(3)-P.L. 86-36

9/23/2010

(TSUO) He is a futurist. The scientist depicted in the white smock on the mural at the entrance to OPS 2B is Bob Hermann. Few other people in the country have Dr. Hermann's insight into the future of the intelligence community.

(TSUO) He is very opinionated and tells it "like it is". He will be a very interesting speaker.

(TSUO) For the sports fan, he was a pitcher on the Iowa State University baseball team which we believe won the national championship.

(TSUO) Stay tuned for further details from the S&ES Luncheon '96 committee: [redacted] co-chairs. (b)(3)-P.L. 86-36

(TSUO) S&ES members will be given priority on ticket sales.

(TSUO) DR. HERMANN'S BIOGRAPHY:

(TSUO) Dr. Robert J. Hermann was elected Senior Vice President, Science and Technology at United Technologies Corporation in July 1992. In this position, Dr. Hermann is responsible for assuring the development of the company's technical resources and the full exploitation of science and technology by the corporation. He also has responsibility for the United Technologies Research Center.

(TSUO) Dr. Hermann joined the company in 1982 as Vice President, Systems Technology in the Electronics sector and later served in a series of assignments in the Defense and Space Systems groups prior to being named Vice President, Science and Technology at United Technologies Corporation in March 1987.

(TSUO) Dr. Hermann served 20 years with the National Security Agency with assignments in research and development, operations and NATO. In 1977, he was appointed principal Deputy Assistant Secretary of Defense for Communications, Command, Control and Intelligence. In 1979, he was named Assistant Secretary of the Air Force for research, development and logistics and in parallel was Director of the National Reconnaissance Office. In 1981, he was named special assistant for intelligence to the Under Secretary of Defense for Research and Engineering.

(TSUO) He received B.S., M.S. and Ph.D. degrees in electrical engineering from Iowa State University.

(TSUO) Dr. Hermann is a member of the President's Foreign Intelligence Advisory Board; the Defense Science Board; the National Academy of Engineering; the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology; the National Research Council Commission on Physical Sciences, Mathematics and Applications; and the National Society of Professional Engineers Industry Advisory Group. He is a member of the Board of Directors for Draper Laboratories, and the American National Standards Institute; Board of Trustees for the Hartford Graduate Center.

b. (TSUO) Signals Analysis Association Presentation Announced

[redacted]

"Some Preliminary Results from the [redacted] (b)(3)-P.L. 86-36

[redacted]

Spring '96 MiniSCAMP on the Internet ~~(FOUO)~~"

Wednesday, April 3rd 1996
starts 9:15 a.m.
Friedman Auditorium

The presentation is CLASSIFIED.
All green, gold and black badged personnel are invited to attend.

~~(FOUO)~~ ABOUT THE PRESENTATION AND SPEAKER:

~~(C CCO)~~ This talk will present some preliminary results and some lessons learned from the Spring '96 MiniSCAMP on the Internet that was held from 12 Feb 96 to 22 March 96 at IDA/CCS in Bowie MD. MiniSCAMPs are working conferences aimed at producing results on important Agency problems. The purpose of this MiniSCAMP was to develop techniques to examine and work with large sets of data containing computer communications. The large data set that was chosen was approximately 10 Gbytes of data from a day in the life of the Internet. The MiniSCAMP also served as a tool to educate a number of people that had no previous experience with computer networking. Thirty-five people from across the Agency and GCHQ participated.

(b)(3)-P.L. 86-36
(b)(6)

[redacted]

c. (U) Crypto-Linguistic Association (CLA) Call for Nominations

~~(FOUO)~~ The Crypto-Linguistic Association (CLA) is accepting nominations for the Sydney Jaffee and Capt. Rochefort Awards. These awards are made to two outstanding linguists each year, one civilian and one military. The civilian linguist's award is the Sydney Jaffe Award. The military linguist's award is the Capt. Rochefort Award. Candidates may be nominated by any three members of the cryptologic community, by the chairman of the Language Career Panel, or by any supervisor at division (or equivalent) or above. Persons in the Service Cryptologic Element organizations outside of NSA may also be nominated at the operations office level (or equivalent) or above.

~~(FOUO)~~ Nominations must be in writing. In addition to the name, grade or rank, and organization of the candidate, a write-up of approximately 2 to 4 typed pages is required, detailing the candidate's accomplishments in the language field and specifying how the individual contributed to the cryptologic community's mission. For details, see the official announcement dated 7 February 1996.

All nominations must be submitted by 12 April 1996 to:

Chairman, CLA Jaffe/Rochefort Award Committee
ATTN: [redacted]
National Security Agency
Fort George G. Meade, MD 20755-6000

Questions about the nomination process should be directed to [redacted]

[redacted]

(b)(3)-P.L. 86-36

[redacted]

****
//////////

5. TECHNICAL HEALTH

a. (FOUO)

(FOUO) The Z Technical Health Award was formally established by Chief, Z in December, 1995 (see Z Regulation No. 30-2) "to recognize Agency personnel who have made outstanding contributions to the technical health of Z". These prestigious cash awards, ranging in size up to the maximum of an SPCA, are granted semi-annually to individuals and teams for special acts or accomplishments above and beyond the recipients' regular duties.

(FOUO) Nine recipients of Z Technical Health Awards for the 2nd Qtr FY-96 were recognized by Chief, Z in a special awards ceremony on 3 April. Names of seven of the nine awardees are:

[redacted] (b)(3)-P.L. 86-36

(FOUO) The Z Group Technical Career Advisory Board (TCAB), Z's technical track oversight body, is the deliberative body for the Award and is responsible for forwarding a list of its recommendations to Chief, Z for action. Nominations for this award may be generated by individuals within Z, by Z technical health entities, such as the various Office Technical Health Boards (OTHB), the Technical Track Review Panels, or the TCAB itself.

****

b. (FOUO) THE RSA PUBLIC KEY CRYPTOSYSTEM

By: [redacted] (b)(3)-P.L. 86-36

Section 1: Introduction

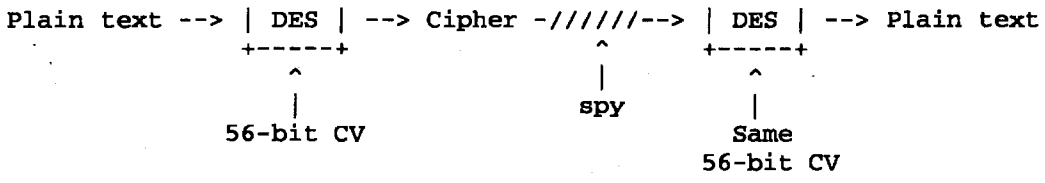
(FOUO) There are two general categories of cryptographic devices: "secret-key" and "public-key". Secret-key devices require that both the sender and receiver agree on a "key" or cryptovariable (CV) before secure communications can be initiated. The security of a secret-key system is the CV. If communication is to be secure, then the CV must remain a secret between the sender and receiver.

(FOUO) A familiar example of a secret-key system is the Data Encryption Standard (DES). In DES, the same method (algorithm) and CV are used for both encryption of plain text, and decryption of messages. The security of DES lies entirely in the 56-bit CV.

(b)(3)-P.L. 86-36

+-----+ +-----+ Original

[redacted]



(~~FOUO~~) Figure 1: DES, A secret-key system.

(~~FOUO~~) Benjamin Franklin is believed to have said that "Three can keep a secret if two of them are dead." Using a secret-key system requires that the sender, receiver, and the courier who facilitates the exchange of cryptovariables, keep their mouths shut. Clearly the sender and receiver want secure communication. The underpaid courier, however, might accept a bribe or otherwise be convinced to disclose the cryptovariable, rendering the boss' communications open to eavesdroppers. Public-key systems take the courier out of the loop.

(~~FOUO~~) In a public-key system, the keys used for encryption are different from those used for decryption. Furthermore, it is very difficult or (ideally) impossible to recover decryption keys given only encryption keys. These systems are called public-key because the encryption key can be made public. The corresponding decryption key, however, is kept secret.

Section 2: Just Enough Math

(~~FOUO~~) Each positive integer can be classified as being either prime or composite.

> A prime number is an integer greater than 1 that cannot be evenly divided by any positive integer except itself or 1. An integer greater than 1 that is not prime is called a composite number.

The first few prime numbers are 2, 3, 5, 7, 11, 13, and 17. Are these all of them? No! There are infinitely many prime numbers. Further, every composite number can be written uniquely (up to the ordering of the factors) as a product of prime numbers.

(~~FOUO~~) Given two numbers, a and b, the greatest common divisor, or "gcd" of a and b, is the largest positive number that evenly divides both a and b. If the largest number that evenly divides both a and b is the number 1, then we call a and b "relatively prime" numbers.

(~~FOUO~~) We say that two numbers are of the same "parity" if they are both even or both odd. For example, the numbers 2 and 4 have the same parity while 2 and 5 do not. An algorithm to determine if two numbers have the same parity is to subtract one from the other; if the result is even then the numbers have like parity; if the answer is odd they do not. Formally we could write:

> the numbers a and b have the same parity if and only if we can write the difference (a - b) as some multiple of 2.

(b)(3)-P.L. 86-36

We can easily generalize this notion to what is called "congruence modulo (mod) n" where n is some number larger than 1:

> the numbers a and b are congruent modulo n if
> and only if we can write the difference (a - b)
> as some multiple of n.

In this article, we will denote the statement "a is congruent to b modulo n" as

a == b (mod n).

For example:

23 == 2 (mod 7)

because we can write the difference (23 - 2) as

(23 - 2) = 21 = (3 * 7).

Another example is

37 == 2 (mod 7)

because

(37 - 2) = 35 = (5 * 7).

~~(FOUO)~~ In fact, a number is congruent mod n to every other number whose distance away on the number line is a multiple of n. When the number a is divided by n, the remainder r is congruent to a modulo n. This is true because (using long division) we can write:

a = (quotient * n) + r

which shows that (a - r) is a multiple of n. Since the remainder is always larger than or equal to 0 and less than n, it is called the "least nonnegative residue of n."

Section 3: The RSA Algorithm

~~(FOUO)~~ The RSA system is named after R. Rivest, A. Shamir, and L. Adleman. RSA depends on the assumption that it is easy to find large prime numbers (integers greater than 1 that cannot be evenly divided by any positive integers except itself and 1), but if they are multiplied together it is very hard to retrieve the prime factors given only the product. In practice, the prime numbers involved here are at least 256-bits long. Even with much smaller numbers we can see that the problem of recovering factors is harder than finding primes. For example, it is not too hard to show that 113 and 11,831 are prime, however if you're given the number 1,336,903 to factor, it's not immediately clear how you would figure out that 1,226,903 = 11,831 * 113.

(b)(3)-P.L. 86-36

9/23/2010

~~(FOUO)~~ Typical messages in the RSA system are cryptovariables for secret-key systems like DES. Before someone can use the RSA system, they must generate a "key pair". Each user finds two large prime numbers p and q, and a number E that is relatively prime to the product Z = (p - 1) * (q - 1); i.e., E has no common factors with either (p - 1) or (q - 1). The user now makes the following pieces of information public: the number E, and the product N = p * q.

Public Key: (E, N).

The user now finds a number D that makes the following congruence true

(E * D) == 1 (mod Z).

This is very easily done by computing gcd(E,Z) with the extended Euclidean algorithm. Finally, the user destroys the numbers p, q, and Z and stores the number D in a safe place.

Secret Key: (D, N).

~~(FOUO)~~ Bob wants to use the RSA system. Bob selects the two primes

p = 113 and q = 227

(Note, we are using small primes here for instructional purposes.) Multiplying p and q together we have

N = P * q = 113 * 227 = 25651

and

Z = (p - 1) * (q - 1) = 112 * 226 = 25312.

Bob now picks E = 3 and checks that it is relatively prime to Z = 25312. Finally, Bob solves the equation

(3 * D) == 1 (mod 25312)

for D and finds that D = 16875; i.e,

(3 * 16875) - 1 = (2 * 25312).

Bob's key generation is complete. Bob destroys p, q, and Z, publishes

Bob's Public Key: (E, N) = (3, 25651)

and stores his secret key

Bob's Secret Key: (D, N) = (16875, 25651)

in a safe place.

(U) Say Alice, another user of the RSA system, wants to send an encrypted 56-bit DES cryptovariable M to Bob. Alice looks up Bob's public key (E,N), raises the message M to the E-th power and sends the least nonnegative residue (remainder) modulo N

(b)(3)-P.L. 86-36

$$C = M^{E} \pmod{N}$$

to Bob. Suppose the DES cryptovariable was M = 5150. Then, Alice would compute

$$5150^{3} \pmod{25651} == 18228$$

and send the cipher message C = 18228 to Bob.

(U) Bob uses his secret key (D,N) to decrypt cipher

$$18228^{16875} \pmod{25651} == 5150$$

to the original plain text. This works because of a mathematical theorem from the 1600s called "Fermat's Little Theorem" that states:

If p is a prime number then for any number a,

$$a^{p} == a \pmod{p}.$$

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

c. (U) CRYPTOLOGIC ALMANAC

More on the Bombe

(U) The Cryptologic Almanac announcement that the

(b)(3)-P.L. 86-36

[redacted]

World War II cryptanalytic Bombe had returned to the National Cryptologic Museum has sparked interest in how this piece of equipment got its name. Correspondents on ENLIGHTEN have quoted the most popular theories on this, but the truth is--nobody knows for sure.

(U) Among the items of lore passed down from our cryptologic forefathers and foremothers was that the Bombe got its name because it ticked like a time bomb when it ran. The problem is that there is no definite source for this story; it's just one of those things "everybody knows." Never having heard one, I wonder what a time bomb sounds like and how "everybody knows" that, too. (Don't bother sending me one--I'm not THAT curious about the sound!)

(U) David Kahn, in his excellent book _Seizing the Enigma_, says that members of the Polish Cipher Bureau, who originated the concepts for the processing machine, gave it this nickname because they came up with some of the ideas while enjoying a frozen "bombe," a popular dessert.

(U) Last week, one of the truly great figures of scientific intelligence in World War II visited the National Cryptologic Museum. This was R.V. Jones, author of _The Wizard War_. While viewing the museum's exhibits, he mentioned he had worked with the famous mathematician Allen Turing on the Bombe design. I asked him if he knew how the Bombe got its name. He gave me an immediate and accurate answer--he said he didn't know.

(U) I suspect that the designation "bombe" was simply a covername. They had to call it something, and "bombe" had a military sound to it.

(U) However the name arose, everyone is invited to come and see the Bombe on display in the National Cryptologic Museum. Museum hours are 0900-1500 on weekdays and 1000-1400 on Saturdays. (The museum will have special hours for NSA's Family Day, but more about that in a future Cryptologic Almanac.)

~~(FOUO)~~ [David A. Hatch, Director, Center for Cryptologic History, [redacted]

(b)(3)-P.L. 86-36

***

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

b. (U) LAST MONTH'S PUZZLES

Puzzle #1: Birthday Ununiqueness

(U) I was sitting around with my friend Waldo and his grandfather Mortimer last week, and the topic of birthday surprises came up. Mortimer mentioned that one of the greatest surprises that he has had involved his grandfather, who happens to have the same birthday that Mortimer has. One year the family was celebrating this double birthday, and during the events Mortimer proudly mentioned to his grandfather that not only had he just turned as old as the last two digits of the year he was born in, but he was also a prime number of years old, and each of the two digits making up his age was also a prime. Mortimer was floored when the older man thought for a second, turned to him, and said that the same thing had just happened to him! What year did this occur, and how old had Mortimer and his grandfather just turned?

Answer:

(U) It's clear that Mortimer had to have been born in the 1900s, and his grandfather in the 1800s. If Mortimer was born in 1900+x and his grandfather in 1800+y, then 1900+2x=1800+2y (the year this happened), and so y=x+50. Now any odd prime number plus an odd number must be even and greater than 2, and so not a prime, hence Mortimer must have been 20-something. But 25 and 27 are not prime, so Mortimer must have been 23, and so his grandfather was 73 (which is indeed also prime). It follows the year was 1900+2*23=1946.

~~(TOUO)~~ Correct answers were received from: (b)(3)-P.L. 86-36

[redacted]

Puzzle #2: Fast Answer

(U) I was sitting around with my friend Waldo, his nephew Spike, and Spike's friend Molly recently. I happened to have two tickets to a new movie in my pocket that I had just purchased, and I mentioned this and noted that there were two four-digit numbers on the tickets and that the sum of all 8 digits was 25. Waldo asked if any digit appeared more than twice out of the 8, which I answered. Spike then

[redacted] (b)(3)-P.L. 86-36

asked if the sum of the digits of either ticket was equal to 13, which I answered also. Much to my surprise, Molly immediately told me what the two numbers were. What were they?

Answer:

(U) What Molly realized was that the tickets were consecutively numbered. If the tickets were numbered abcd and abc(d+1)and my answer to Spike's question had been yes, the only conclusion, Molly could have reached would have been that a+b+c+d=12, and regardless of my answer to Waldo's question, there would not have been a unique solution. So my answer to Spike's question must have been no, and it follows that the tickets could not have been numbered in this manner. If the numbers were abc9 and ab(c+1)0, we'd have 2a+2b+2c+10=25, and so 2(a+b+c)=15, which is impossible. If the numbers were ab99 and a(b+1)00, we'd have 2a+2b+19=25 or a+b=3, leading to the four possibilities 0399 and 0400, 1299 and 1300, 2199 and 2200, 3099 and 3100. Of these three of them would have had me answer "yes" to Waldo's question, and only the pair 1299 and 1300 would have had me answer "no". It follows that these were my ticket numbers.

(FOUO) Correct answers were received from:

[redacted]

****

(b)(3)-P.L. 86-36

c. (U) NEW PUZZLES

(U) April puzzle. Answer either or both. Send answers to [redacted]

[redacted]

(U) Puzzle #1: Cheese and Fleas

(U) Waldo, Basil, Molly, two wedges of cheddar, two wedges of mozzarella, and Rufus the dog are going to the annual Cucumberland cheese competition and dog show. Waldo's little sports car can only seat two objects at a time; Waldo, Basil, and Molly can drive the car. If Waldo is not around, Basil will eat the cheddar. If Basil is not around, Waldo will eat the mozzarella. If Molly is not around, Rufus will eat the cheese and bite Waldo and Basil. Can they all get to Cucumberland without anything bad happening? If so, what's the smallest number of trips needed, and who and/or what goes in each trip (each way counts as one trip)? (Please note, each wedge of cheese counts as 1 object.)

(U) Puzzle 2: Rumor Mill

(U) Waldo is having a party and has 50 guests, among whom is his brother Basil. (Waldo is not counted as one of the 50 guests.) Basil starts a rumor about Waldo; a person hearing this rumor for the first time will then tell another person, chosen uniformly at random, the rumor, with the exceptions that no one will tell the rumor to Waldo or to the person they heard it from. If a person who already knows the rumor hears it again, they will not tell it again. What is the probability that everyone, except Waldo, will hear the rumor before it stops propagating?

****

(b)(3)-P.L. 86-36

[redacted]

//
##

(U) EDITORIAL CORNER

REMINDER: Submissions for the May issue are due by April 25th.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

(b)(3)-P.L. 86-36

\\\

TOP SECRET//COMINT

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:20
(U)PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
May 1996

[redacted] (b)(3)-P.L. 86-36

//
****

(FOUO) TABLE OF CONTENTS:

1. (U) CA Perspective
2. (U) Calendar of Events
3. (FOUO) KRYPTOS News
4. (U) Technical Health
5. (U) Action Line
6. (U) Cryptologic History
7. (U) Community Service
8. (U) Puzzles
9. (U) Editorial Corner

//

1. (C) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature [redacted] [redacted] (b)(3)-P.L. 86-36

~~~~~~

(TSC) Having been outside of Z Group for the past year, I thought it might be useful to offer an INFOSEC perspective on the state of cryptanalysis. In the twenty plus years that I have served at the Agency, I have on many occasions seen our community wrestle with the question of where cryptanalysis was headed and whether its days were numbered. We successfully weathered and, in fact, flourished under the explosion in the commercial cipher machine market which occurred in the early 80's. [redacted]

[redacted] (b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # {61704

[redacted] (b)(3)-P.L. 86-36
~~~~~~

(TSC) In the 90's we have been faced with the challenges of computer networks and the proliferation of strong software cryptography. Though

[redacted]

(FOUO) Despite my pride in what our community has accomplished in the past and my optimism in our ability to make the changes needed to tackle the difficult problems we face today, I believe that we should be concerned about the future. It is not so much the rapid pace of technological advance which worries me. Rather it is a qualitative change that is taking place, namely the role that cryptography plays in our society. Cryptography will soon be a commodity with impact far beyond the traditional domain of government and classified information. This change is the inevitable result of the spread of information technology. Computers are gradually invading every aspect of our lives. As a result, the security concerns that make us use locks and keys and other physical protections will soon drive us to demand information security devices. We will be carrying crypto-tokens and they will not only replace credit cards for financial transactions but will affect every aspect of our daily lives >from access to our home and office to medical services and records, entertainment, and personal communications.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(FOUO) We have already reached the point where important public assets such as the telephone system, air traffic control network, power grid, and banking system are highly automated. Our nation faces a major crisis in providing the security infrastructure required to, on the one hand, protect our personal affairs from criminal activity, and on the other, secure our public assets from more serious threats. In doing so, we must somehow balance the competing interests of economic health, personal privacy, law enforcement, and intelligence.

(S-CCO) This challenge is greatly complicated by two fundamental factors. [redacted]

[redacted]

(S-CCO) We must improve our performance of the INFOSEC mission and to do so will require us to change our way of doing business. [redacted]

(b)(1)
(b)(3)-P.L. 86-36

At the same time I am convinced that the two missions are intrinsically linked and it would be unwise to try to accomplish them independently. Simply producing decrypts will not assure our national security. Fortunately NSA cryptanalysts have a tradition of moving forward in the face of overwhelming challenges. And if WE can't tackle the technical problems and develop the strategy to meet this challenge, who can?

(b)(3)-P.L. 86-36

[redacted]

2. (U) CALENDAR

May 2	IAI Twenty-Fifth Anniversary Luncheon
May 9	S&ES Symposium (R&E Auditorium, 1000)
May 13-17	ACE 1996 at CCS in Bowie.
May 16	CISI General Meeting and Presentation, "Improving Technology Insertion and Other Information Technology Issues", [redacted], Chief J, and [redacted] (Friedman, 0930)
May 21-22	CA PQE
May 28	CA-305 Begins
May 30	MATHFEST '96 and CMI Banquet

(b)(3)-P.L. 86-36

PLAN AHEAD

June 4	CLA Banquet, "Should We Hate the Media?", [redacted] (Canine Suite, 1130-1330)
June 6	Pen and Cursor Luncheon, "Freelance Writing", [redacted] (Canine Suite, 1200-1400)
June 18	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)
June 18	Science & Engineering Society, June Symposium, (R&E, 1300)
June 26	KRYPTOS Talk, Cecil Phillips, "More on the VENONA Releases", (Cryptologic Museum, 1000)
Sep 17	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)
Nov 19	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)
Nov 18-22	CONSCRYPT '96, at DSD

(b)(6)

3. (U) KRYPTOS SOCIETY NEWS

a. (U) Literature Contest Announcement

(TSC) Sponsored by KRYPTOS, the professional society for cryptanalysts, the competition is open to all personnel at NSA, to personnel on field assignments, and to retirees (consistent with security considerations). Papers may treat any topic in the broad category of professional cryptanalytic literature, including:

(b)(3)-P.L. 86-36

[redacted]

_____ attacks and techniques relating to cryptanalytic problems;
_____ cryptanalytic research;
_____ history of cryptanalysis;
_____ other subjects relating directly to cryptanalysis, e.g., target studies, cryptologic trends from the point of view of cryptanalysis, or computer support of a cryptanalytic problem.

(U) Submissions may be written specifically for the competition. They need not be, however. Papers written between July 1, 1995 and June 30, 1996 are eligible. Entries may carry a classification of up to TSC. Compartmented papers will be considered only in extraordinary cases. Papers should be submitted with two cover sheets: the name(s) and organizations(s) of the authors(s) and title on one sheet, and only the title on the other, to facilitate impartial judging.

(U) The judges will consider the following criteria:

_____ Is the paper an original discussion of a cryptanalytic subject?

_____ Is the paper well written? Is the subject presented well? Can a reader with a suitable technical background but unfamiliar with the subject understand the paper and, by reading it, gain knowledge about the subject?

_____ Does the paper constitute an important addition to the body of cryptanalytic literature?

(U) The judges will determine up to three winners: cash prizes of $125, $75, and $50 will be awarded to first, second, and third place winners. The judges may designate papers to be worthy of honorable mention. KRYPTOS hopes to publish some of these winning papers in Agency professional journals.

(FOUO) To enter, please submit four copies of your paper to [redacted]. The deadline for entries is July 1, 1996. The competition results will be announced at the KRYPTOS luncheon in October 1996.

b. (U) VENONA Summer Presentation

(U) The KRYPTOS Society is pleased to announce that Cecil Phillips will give a talk in June at the NSA Cryptologic Museum on the VENONA material. This will give us an opportunity to invite retired employees to attend, as the talk, and exhibit currently on display, are, of course, unclassified.

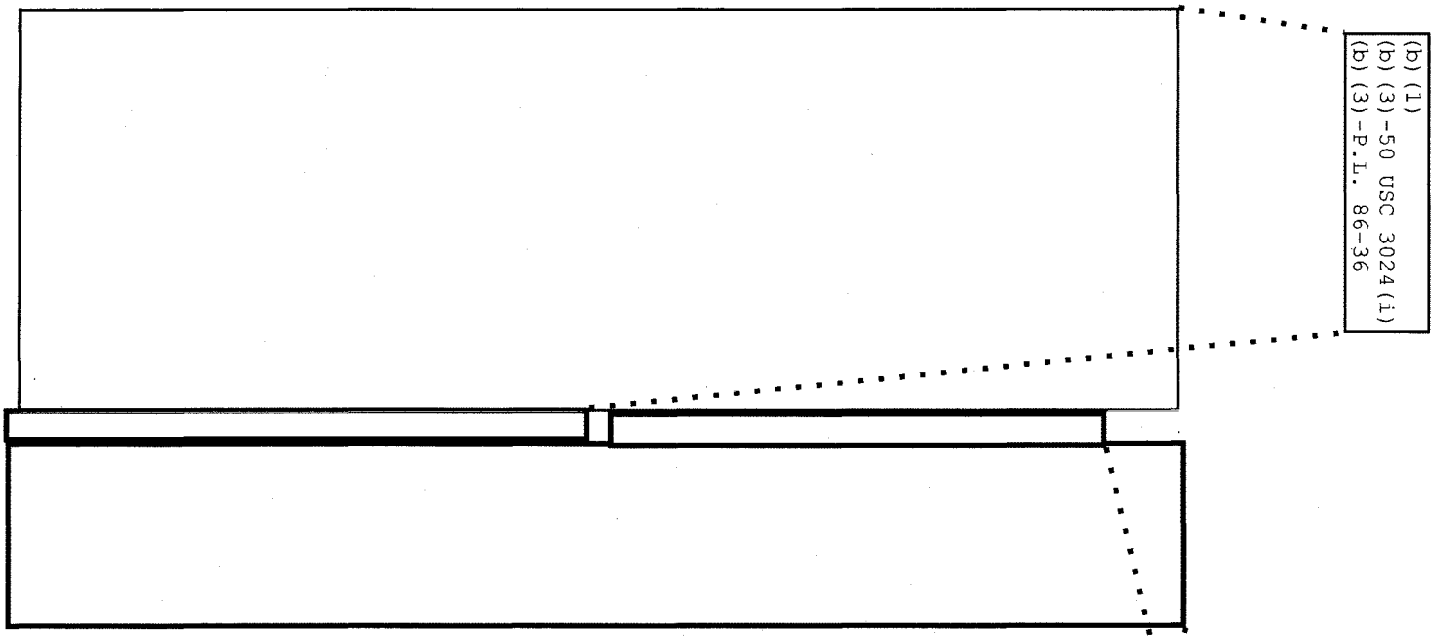
(b)(3)-P.L. 86-36

4. (U) TECHNICAL HEALTH

a. (U) S&ES Symposium

(S) The speakers will be a team composed of [redacted] and [redacted] The subject of the team's presentation will be:

[redacted]



(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

b. (U) CISI Presentation

~~(FOUO)~~ [redacted] and [redacted] co-chairs of the newly established Technology Insertion Board, will discuss plans to improve the way technology and systems are acquired or developed into products for broad-based use within NSA. They will relate key findings >from a DDO/DDT-commissioned study; provide the audience with helpful hints to increase the chance of developing an easily integrated and broadly used product; and introduce the role of the Technology Insertion Board in the improvement process.

(U) Following the briefing on Technology Insertion, the speakers will provide information on other forums established to address Information Technology issues. A question and answer period covering all topics addressed will conclude the presentation.

(U) The presentation is open to all cleared personnel. For those who cannot make the trip to the OPS campus, the presentation will be broadcast on NEWSMAGAZINE Channel 16 and will be videotaped. Contact the CISI secretary to borrow the tape for viewing in your office.

//

5. (U) ACTION LINE

(U) QUESTION: "How are members of Z Office-level-and-above promotion boards chosen? How are the chairmen chosen?

(U) ANSWER (provided by M3Z)

~~(FOUO)~~ M3Z goes out with a memo asking for nominations from each Office to sit on the new board. Each Office makes submissions and the list goes to Chief of Z. He will select from the list and also selects a Chairman, a female rep and a minority rep. Each board member serves for 2 cycles. They must be one grade higher than the grade for which they serve. The 15 board is made up of Office Chiefs due to grade level. Feel free to

(b) (3)-P.L. 86-36

call M3Z at [redacted] for additional information about the boards.

****
//////////

6. (U) CRYPTOLOGIC HISTORY (b)(3)-P.L. 86-36

a. (U) Cryptanalysis Postage Stamp

(U) A 29-cent postage stamp was issued in 1992 to commemorate cryptanalytic successes in WWII. The design includes a page of cipher (PURPLE can be seen at the top), a red pencil, and a set of headphones. There is a line of text at the bottom of the stamp which reads "Allies decipher secret enemy codes, 1942". The stamp is part of a sheet of ten stamps commemorating various war-related events that took place in 1942. This sheet is still available at face value from the U.S. Postal Service. [redacted] will be ordering a quantity of these sheets later this month. If you are interested, send a message to him at [redacted] indicating the number of sheets you want.

****
//////////

7. (U) COMMUNITY SERVICE

a. (U) CLA Banquet Announcement (b)(6)

(U) The Crypto-Linguistic Association is very fortunate to have for its guest speaker this year [redacted] author, Washington editor of the Atlantic Monthly, National Public Radio commentator and Asian expert. He will speak on the topic of his latest book, "Should We Hate the Media?"

(U) In addition, the winners of the 1995 Jaffe, Rochefort, and [redacted] Awards will be announced at the banquet. Come celebrate 31 years of fellowship and linguistic adventure and excellence!

(U) Below is additional information about the keynote speaker: (b)(3)-P.L. 86-36

Harvard Crimson President, 1969
Harvard University (B.A.), 1970
Queens College, Oxford (Rhodes Scholar, 1970-1972)
Washington Monthly Editor, 1972-1974
Texas Monthly Editor, 1974-1976
Chief Speechwriter for President Jimmy Carter, 1977-1979
Washington Editor of the Atlantic Monthly, 1979-present
One of five finalists for National Book Critics Circles Award for general non-fiction, (National Defense), 1982
American Book Award in general non-fiction, (National Defense), 1983
National Commentator, National Public Radio, 1987-present

He has written the following non-fictional works:
The Water Lords, 1971
Who Runs Congress, 1972
National Defense, 1981
More Like Us: Making America Great Again, 1989
Japanese Education: What Can It Teach American Schools, 1990
Looking at the Sun, 1994

[redacted]

[redacted] has just written another book (and the subject of his speech)--"Breaking the News: How the Media Undermine American Democracy." (b) (6)

Tickets ($12.95) will be on sale until 28 May and may be purchased >from any of the members listed below:

[redacted] (b) (3)-P.L. 86-36

****

//////////

8. (U) PUZZLE CORNER

a. (U) Solutions to Previous Puzzles

Puzzle #1: Cheese and Fleas

Waldo, Basil, Molly, two wedges of cheddar, two wedges of mozzarella, and Rufus the dog are going to the annual Cucumberland cheese competition and dog show. Waldo's little sports car can only seat two objects at a time; Waldo, Basil, and Molly can drive the car. If Waldo is not around, Basil will eat the cheddar. If Basil is not around, Waldo will eat the mozzarella. If Molly is not around, Rufus will eat the cheese and bite Waldo and Basil. Can they all get to Cucumberland without anything bad happening? If so, what's the smallest number of trips needed, and who and/or what goes in each trip (each way counts as one trip)?

Answer:

Yes, they can do it, and the smallest number of trips is 17. There are essentially two ways of doing this in 17 steps. One is:

Molly and Rufus; Molly; Molly and cheddar; Molly and Rufus; Waldo and cheddar; Waldo; Basil and Waldo; Basil; Molly and Rufus; Waldo; Basil and Waldo; Basil; Basil and mozzarella; Molly and Rufus; Molly and mozzarella; Molly; Molly and Rufus.

The other method is to do this in reverse. Another way of looking at it is that we're swapping cheddar and mozzarella, Basil and Waldo, since from the point of view of the other restrictions, this changes nothing.

Correct answers were received from [redacted] and [redacted] (b) (3)-P.L. 86-36

[redacted]

Puzzle 2: Rumor Mill

Waldo is having a party and has 50 guests, among whom is his brother Basil. Basil starts a rumor about Waldo; a person hearing this rumor for the first time will then tell another person, chosen uniformly at random, the rumor, with the exceptions that no one will tell the rumor to Waldo or to the person they heard it from. If a person who already knows the rumor hears it again, they will not tell it again. What is the probability that everyone, except Waldo, will hear the rumor before it stops propagating?

Answer:

Let person one be the initiator, and person m>1 be the m'th person to hear the rumor. Then the probability that person m will give the rumor to a person who hasn't heard it yet is (48-(m-2))/48, since there are 48 people who can hear the rumor, and of these, m-2 have already heard it. Thus the probability that the rumor will propagate to everyone is the product (50-2)/48 * (50-3)/48 * ... * (50-49)/48, which equals 48!/(48^48).

Correct answers to problem #2 were received from [redacted]

[redacted]

b. (U) May Puzzles. (b)(3)-P.L. 86-36

(U) Answer either or both puzzles, and send solutions to [redacted]

[redacted]

Puzzle 1: Turophile Teaser

The Cucumberland grocery has six cheese wedges of different sizes, weighing 15, 16, 18, 19, 20, and 31 pounds. Five wedges are cheddar, and only one wedge is mozzarella. Waldo bought two wedges of cheddar, and Basil also bought cheddar, but twice as much by weight as Waldo. How much does the mozzarella wedge weigh?

Puzzle 2: Island Quandary

Waldo mentioned the problem they had getting to the Cucumberland fair recently (see last month's puzzle), and Mortimer recalled a similar occurrence from his days as a boy. It seem that three couples staying on an island wanted to cross the water using a boat that could only hold two people at a time. In those days, it was considered improper for a woman to be with a man who was not her husband unless her husband was also present. How many trips were required? Each way counts as one trip.

9. (U) EDITORIAL CORNER

(b)(3)-P.L. 86-36

REMINDER: Submissions for the June issue are due by May 24th.

PLEASE NOTE: All submissions must be in ASCII format, and, with the

[redacted]

implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

(b)(3)-P.L. 86-36

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

\\\

~~(S)~~ POC: [redacted] info
(U) *Last Modified: 10/30/2002 11:42:20*
(U)PE EXTERNAL PAGE

THE CLASSIFICATION OF THIS NEWSLETTER IS ~~TOP SECRET UMBRA~~

(b)(3)-P.L. 86-36

****
* TALES OF THE KRYPT *
****
June 1996

//
****

~~(FOUO)~~ TABLE OF CONTENTS:

1. (U) CA Perspective

2. (U) Calendar of Events

3. ~~(FOUO)~~ CACP News

4. (U) KRYPTOS News

5. (U) Technical Health

6. (U) Cryptologic History

7. (U) Puzzles

8. (U) Editorial Corner

(b)(3)-P.L. 86-36

//

1. ~~(S)~~ PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature [redacted] Chief Z03.

~~~~~~

CRYPTANALYSIS FROM BOTH SIDES OF THE FENCE (U)

(U) Let me say first that I was quite surprised and flattered to be asked to write for this publication. My instructions have been to pick any CA-related topic and to make it brief. For those of us who have worked at the Agency for three decades, there are of course countless "war" stories but I thought that I would focus on the issue of change, and the effect that change is going to have on us functionally and psychologically.

~~(S)~~ At the risk of oversimplifying, cryptanalysis from post-WWII to the late 80's was a relatively stable process in terms of culture, technology, targeting and definition. Of course there has been growth over these 40+ years, but it has tended to be steady growth prompted by a reasonably predictable target set and a general feeling that, in the CA community, we understood what cryptanalysis was and how to continue doing business as usual. With the dissolution of the Soviet Union and the rapid evolution of complex and ubiquitous telecommunications

Approved for Release by NSA on 09-28-2023, FOIA Case # {61704
~~~~~~

technology, we have had to deal with a sudden redefinition of cryptanalysis itself. Before I plunge into the future, allow me to reminisce a bit to give you some idea of the flavor of one of my early experiences and the role that it played in keeping me enthusiastic about cryptanalysis to this day.

~~(S)~~ For me, cryptanalytic life in the 70's was good. The goals were clear (at least in my naive view at the time), the issues were simple and morale was high. The adversary technology we were up against was far simpler than that confronting us today, traffic volumes were low and cryptanalytic problems were difficult but more than occasionally tractable. Work hard, work together, successfully attack tough problems, make decrypts, win big. No problem.

~~(TSC)~~ My first recollection of working in such an idyllic environment was in G41 in the early and mid 70's. For those of you too young to remember, one of the predominant problems at hand was the family of

[redacted] (b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

~~(TSC)~~ The working conditions at the time, especially in the tube room, were something far more akin to a MASH unit than the pristine environment of today. (ED. NOTE: For those who may not remember them, tube rooms were where the computers resided, and you had to sign up to use them - desktop computers were unknown at the time!) We blindly worked endlessly long hours (or so we say now), with food remnants and overflowing ashtrays very much the order of the day. I can remember dozing off at the tube at 3 AM while waiting for an important [redacted] or other program to complete and then feeling totally energized when I "hit it big". These were the greatest days, and, if nothing else, they served to motivate me for the rest of my career. If you've had this sort of electric experience, you will know exactly what I mean. While I was very much an ordinary player in an outstanding cast, I was left forever with the belief that I could prevail over tough problems and survive some dark days if need be without getting discouraged. I will forever be in debt to those with whom I worked during those years 1970-1978. One might argue that, in terms of SIGINT bang for the buck, some of the subsequent programs with which I have been associated since then [redacted] (b)(3)-P.L. 86-36 [redacted] However, in terms of contributing to long-term positive professional values, my early experiences in G41 are second to none.

~~(S)~~ Enough nostalgia. If those early years were one side of the cryptanalysis fence, our present and rapidly approaching future are the other and, as a community, we need to be mentally prepared and motivated to successfully tackle a stunning volume and variety of truly daunting technological problems if we are to build on our past level of success and remain relevant in the eyes of our customers. We all have to get used to the reality that cryptanalysis of the future is going to require a far broader range of technical skill coupled with a sophisticated understanding of telecommunications and how to target every facet of the telecommunications path. Cryptanalysis, if defined

[redacted] (b)(3)-P.L. 86-36

"merely" to be the analysis of enciphered communications and nothing more, will become irrelevant without a substantial integration with the [redacted] I believe that, intellectually, we all know this to be true. The big jump is going to be to make the cultural and emotional adjustment necessary to not only force us to organize and function in this new way, but to lead us to do so with the same self-sustaining enthusiasm we brought so successfully to the Cold War cryptanalytic mission.

(U) With skill, experience, belief in the value of the Agency's mission, and sheer force of will, we will prevail over many of the critical problems facing us. Success, after all, is not really all that tough. You decide where you need to go, and then do whatever it takes to get there. The problems of the 21st century will be vastly different >from those of earlier decades, but mental toughness, persistence, risk taking, and aggressive leadership will, as always, be essential ingredients in our productive future. I have had an exceptionally gratifying career and have had the good fortune to work with many fine professionals. My wish is that when each of you look back on your careers, you are left with the same lasting feeling. Good luck.

(b)(3)-P.L. 86-36

****
//////////

2. (U) CALENDAR

June 4 CLA Banquet, "Should We Hate the Media?", [redacted] (Canine Suite, 1130-1330)

(b)(6)

June 6 Pen and Cursor Luncheon, "Freelance Writing", [redacted] (Canine Suite, 1200-1400)

June 18 KRYPTOS Talk, "A Crypto-TA Success Story", [redacted] (Friedman, 1300)

June 18 Science & Engineering Society, June Symposium, (R&E, 1300)

June 26 KRYPTOS Talk, Cecil Phillips, "More on the VENONA Releases", (Cryptologic Museum, 1000)

PLAN AHEAD

Sep 17 KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)

Nov 19 KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)

Nov 18-22 CONSCRYPT '96, at DSD

****
//////////

3. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

[redacted]

a. (U) CAPQE

(FOUO) The 57th Professional Qualification Examination in Cryptanalysis (CAPQE) was given on May 21 and 22. The format was modified slightly this year to make it a two-day (morning only) exam rather than three-days, as it was in past years. Aspirants needed to answer 9 problems out of 16 correctly to pass. The passing rate in previous years has been around one-third, and this year was no exception. Eight out of 24 passed, and scores ranged from a total of 1 right to 15.

****

b. (U) RECENT CERTIFICATIONS

(b)(3)-P.L. 86-36

(FOUO) Congratulations to [redacted] on becoming certified in Cryptanalysis this month!

****

c. (U) NEW CA PROFESSIONALIZATION CRITERIA

(FOUO) We've been announcing its imminent arrival for a while now, but the revised criteria for professionalization in cryptanalysis is almost ready to hit the streets. It has been through all the pertinent channels and is awaiting the signature of the Chief of M8 in order to become an official career development document. We expect to be able to disseminate it in June.

****

d. (U) NEW CRYPTOLINGUISTIC CRITERIA

(FOUO) The Language Career Panel has developed a set of criteria for professionalization as a Cryptolinguist. It, too, is awaiting Chief, M8's signature. If you do bookbreaking, depth reading, or other cryptolinguistic work in a foreign language, this may be the certification for you!

****
//////////

4. (U) KRYPTOS NEWS

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

a. (U) June Talk

(SC) This briefing will include an explanation of the state-of-the-art analysis called Crypto-Traffic Analysis and a description of the successful research project on [redacted]

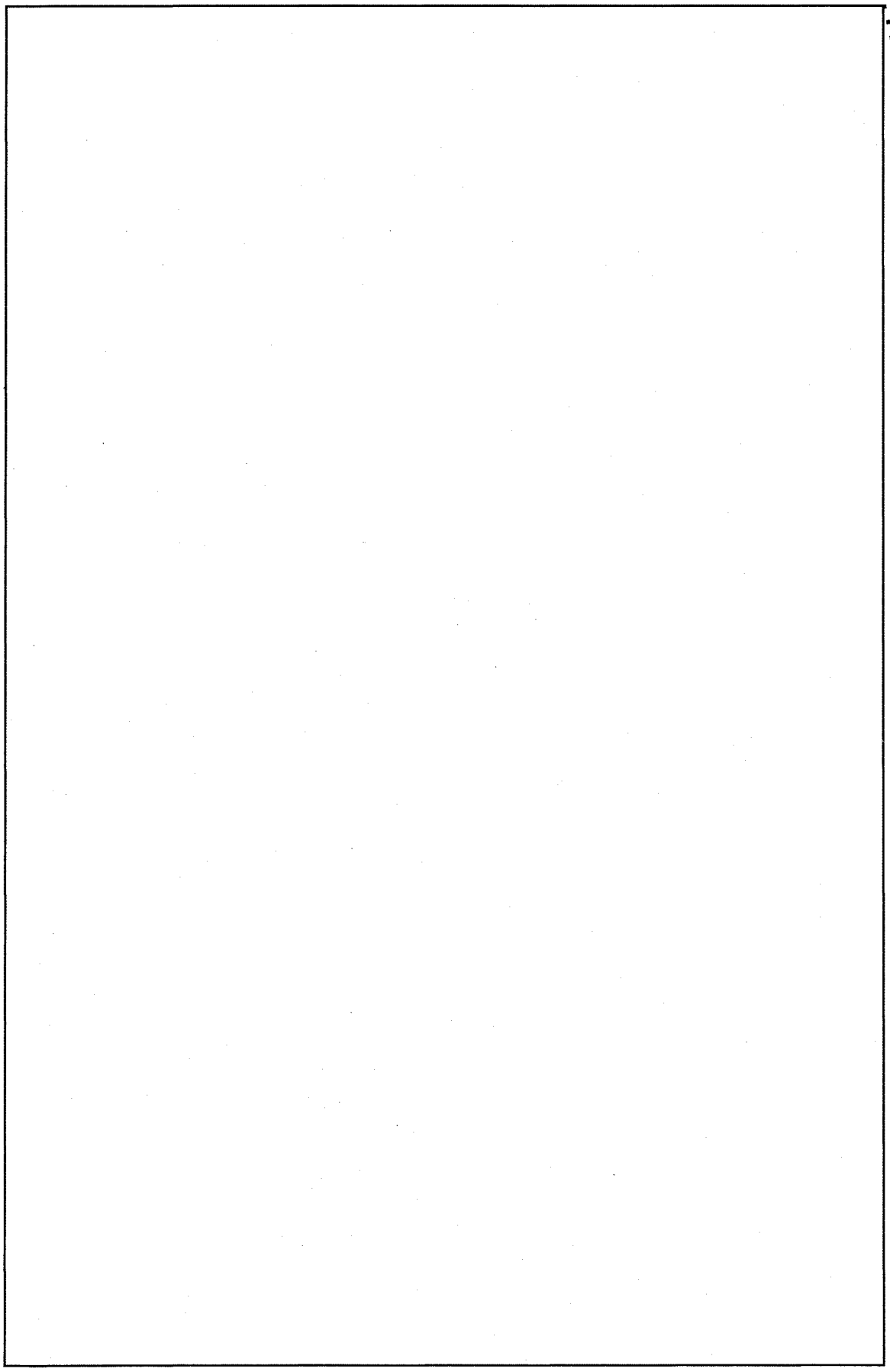
****
//////////

5. (U) TECHNICAL HEALTH

a. (U) CA-305 RECAP

(b)(3)-P.L. 86-36

[redacted]



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

Doc ID: 6823805

6. (U) CRYPTOLOGIC HISTORY

a. (U) BIOGRAPHY - Elizebeth Smith Friedman (1892-1980)
(With thanks to the Cryptologic Almanac)

Elizebeth Smith Friedman - wife, mother, writer, Shakespeare enthusiast, cryptanalyst, and a pioneer in the field of U. S. cryptology - died on 31 October 1980 in Plainfield, New Jersey at the age of 88. Although she is often referred to as the wife of William Friedman, she enjoyed many successes in the field of cryptology in her own right and has been dubbed "America's first female cryptanalyst." In fact, although her husband is credited with numerous contributions to cryptology, it is Mrs. Friedman who introduced him to the field.

Not only did she coauthor a book with her husband and write many other technical papers, she was at times employed by many important agencies whose mission was crucial to matters of national concern and defense. She worked for the U. S. Treasury Department, the U.S. Navy, the U.S. Army, the Canadian government, and following government service - the International Monetary Fund, to name a few. Friedman's career spanned both World Wars, but it was for the period in between that she earned notoriety for her contributions to the international drug and liquor smuggling problems.

Pre College and Early Career Years

Born in 1892 to John M. Smith, a Quaker dairyman, banker, and politician and Sophia Strock Smith, Mrs. Friedman was the youngest of nine children. The special spelling of her name is attributed to Sopha Strock Smith who held a strong passion against Elizebeth ever being called Eliza. With all that is known about her, early childhood information is virtually nil. A frail child, known to have a weak stomach, she battled nausea for all of her life. She was energetic, impatient, and at best strongly opinionated with a disdain for stupidity. She is known to have been a hairdresser, seamstress, and fashion consultant whose talents were often exploited by her friends.

After briefly attending Wooster College in Indiana, she graduated from Hillsdale College in Michigan with a major in English Literature. Having exhibited her interest in the languages, she had also studied Latin, Greek, and German and minored "in a great many other things." Only she and one other sibling were privileged to attend college.

Sometime thereafter, Mrs. Friedman became a professional, probably without a clue that a great career would eventually ensue. Prior to her employment with the Newberry Research Library in Chicago, she was a high school principal for at least a year. A great Shakespeare enthusiast, it is suspected that she was attracted to Newberry because of an "original Shakespeare folio" known to be there. In 1916 while working at Newberry, she was recruited by George Fabyan to work on his 500-acre estate.

Circumstances Surrounding Friedman's Recruitment To Riverbank

Interestingly enough, we are consistently told about Mrs. Friedman's recruitment, but are always left with the burning question of how this all came about. How did Fabyan come to recruit Freidman? What brought Mrs. Friedman to Newberry was her independent search for employment following a lack of leads through an employment agency. By all indications, Mrs. Friedman's job as principal was shortlived because it

(b)(3)-P.L. 86-36

9/23/2010

was not quite what she wanted to do in life. Armed with her enthusiasm for Shakespeare, she was in search of a job that would allow her to do research; she wanted to do something different.

The librarian with whom Friedman interviewed on her first day is credited for having made a phone call that would change the then Miss Smith's life forever. She conveyed, in her telephone conversation, Smith's love for Shakespeare, among other things. Colonel Fabyan, a wealthy textile merchant, was on the line; he would be right over to see Miss Smith. They would meet and discuss the advent of life at Riverbank. At his great estate located in Geneva, Illinois, Miss Smith would assist a Boston woman, Elizabeth Wells Gallup and her sister, with Gallup's attempt to prove that Sir Francis Bacon authored Shakespeare's plays and sonnets using a cipher that was supposed to have been contained within.

Riverbank - An Extraordinary "Think Tank" Facility

Miss Smith had arrived at an extraordinary compound consisting of three parts separated by a highway and river. There were housing facilities for the workers, a villa for the Fabyans, and research laboratories. Not only would there be a department of ciphers, there were laboratories devoted to acoustics, chemistry, and genetics. The staff enjoyed luxurious accommodations, maid service, and elegantly prepared and served meals. Nothing about Riverbank seemed simple. Most everything about the estate was awesome.

The Fabyan's villa, which contained one of two massive pipe organs, was centrally located. It was also home to the many animals Mrs. Fabyan so dearly loved and accumulated over time. The "small zoo" was refuge to purebred dogs and race horses, peacocks, bears, a hive of bees, and a pet chimpanzee known to have "roamed unfettered about the house." Even the grounds were extraordinary. There were sunken gardens, an authentic Japanese garden, a waterlily pond with high and low arched bridges spanning it, a waterfall over a huge rock mound, enormous trees, an antique German windmill, a greenhouse filled with rare plants, a Roman pool, and on the banks of the Fox river - a lighthouse.

Mrs. Friedman's Employment as a cryptanalyst for the U.S. Navy followed in 1923. This led to her employment with the U.S. Treasury Bureau of Prohibition and the Bureau of Customs. The net effect of her career is quite significant and embraces cryptology against international smuggling and drug running in various parts of the world. The smugglers and runners resorted to radio and encoded messages to conduct their operations presumably with a great sense of security. This, however, would become a mistaken notion now that Mrs. Friedman had come to Washington. A more detailed account of her contributions will be dealt with in another almanac article.

During the post WW II era, Mrs. Friedman became a consultant and created communications security systems for the International Monetary Fund.

A longtime Shakespeare enthusiast, Mrs. Friedman and her husband, after retirement from government service, collaborated on what was published as "The Shakespearean Ciphers Examined." It won awards from the Folger Shakespeare Library and the American Shakespeare Theater and Academy. In this document the Friedmans dismissed Baconians such as Mrs. Gallup and Ignatius Donnelly with such technical proficiency and finesse that the book won far more acclaim than others addressing the

(b)(3)-P.L. 86-36

9/23/2010

subject topic. Reflectively, the work that Gallup had done earlier operated on two assumptions: One was that Bacon invented a biliteral cipher, and that the cipher used in the original printed Shakespeare folios employed "an odd variety of typefaces." The Friedmans however, "in a classic demonstration of their life's work," buried a hidden Baconian cipher on a page in their publication. It was an italicized phrase which, using the different typefaces, espoused their final assessment regarding the controversy: "I did not write the plays. F. Bacon." Their finalized document is regarded as the definitive work, if not the final word on the subject.

Following her husband's death in 1969, Mrs. Friedman devoted much of retirement life to compiling a library and bibliography of her husband's work. This "most extensive private collection of cryptologic material in the world" would finally be prepared for the George C. Marshall Research Library in Lexington, Virginia.

Elizebeth Smith Friedman - wife, mother, writer, Shakespeare enthusiast, cryptanalyst, and cryptologist, as evidenced by the life she led, is truly a legend in her own time.

****

(U) Elizabeth Smith Friedman - A Pioneer in the Field of Code-breaking

"OUR OFFICE DOESN'T MAKE `EM, WE ONLY BREAK `EM;" uttered Elizabeth Smith Friedman to a representative of a code building company who came to sell his wares and to tout their precious worth. And "break `em" she did many times over for many years against many targets. Quite admirably, she did all this without the aid of calculators or computers and with only a basic background in mathematics! Her successes led to the conviction of many violators of the Volstead Act during Prohibition Years.

While the 18th Amendment of 1919 forbade the manufacture, sale, import, or export of intoxicating liquors, the Volstead Act forbade the consumption of such beverages. However, prevailing conditions during those days encouraged illegal activity.

Further, as radio equipment became less cumbersome, less conspicuous, and more sophisticated, it afforded the criminal element another means to circumvent the law. To avoid taxes, etc., they smuggled mainly liquor, and to a lesser degree - narcotics, perfume, jewels, and even pinto beans. Rumrunning and bootlegging were typical, and related enciphered communications were passed by persistent anti-prohibitionists to protect their operations.

Anti-prohibitionists provided Friedman and her team of cryptanalysts with "beaucoup" opportunities to hone their cryptanalytic/ codebreaking skills during her employment with the U.S. Treasury Department. She led the cryptanalytic effort against international smuggling and drug running radio and encoded messages which the runners began to use extensively to conduct their illegal operations. Even though early codes were very basic, their subsequent change in complexity and resistance to solution was predicated on the financial success and growth of the operation. The extent of sophistication seemed to pose no problem for Friedman; she still mounted successful attacks against both the simple substitutions and transpositions and the more complex enciphered codes which eventually came into use. While working for the Coast Guard office and the Bureau of Foreign Control during the Prohibition era, she solved over

(b)(3)-P.L. 86-36

12,000 rumrunners' messages.

She also perceived the need to lodge a more dedicated effort against suspected communications. By 1931, she had convinced Congress of the need to create a headquartered, seven-man cryptanalytic section for this purpose. As her cryptanalytic responsibilities began to mount, Mrs. Friedman sensed the need to teach other analysts basic cryptanalytic fundamentals to include deciphering techniques. This allowed her ample time to attack the more atypical new systems as they cropped up and expedited the entire process from initial analysis through to solution. It also allowed her to stay one step ahead of the smugglers.

Although Mrs. Friedman worked closely with her husband as a team, many of her contributions to cryptology were of her own doing. She deciphered many encoded messages throughout prohibition years and solved many notable cases singlehandedly, including some codes which were written in Mandarin Chinese. As has been determined, the complexity or difficulty mattered not. After fifty years at her business, Elizabeth Smith Friedman had indeed proved to be a pioneer in the field of code-breaking.

****
//////////

7. (U) PUZZLES AND PROBLEMS

a. (U) June puzzles: send answers to either or both puzzles to

[redacted]

Puzzle #1: Easy Sum

(b)(3)-P.L. 86-36

Consider the sum:

ABC + DEF + GHI = JJJ

If different letters represent different digits, and there are no leading zeros, what does J represent? (Note, the question only asks for J - there may be several possibilities for the other letters.)

Puzzle 2: Hard Sum

No instructions. When you get the right answer, you'll know it.

HARD + HOKY = LOLY
HOKY + CIA = PYKYL

b. (U) Answers to last month's puzzles (which proved to be very popular):

Puzzle 1: Turophile Teaser

The Cucumberland grocery has six cheese wedges of different sizes, weighing 15, 16, 18, 19, 20, and 31 pounds. Five wedges are cheddar, and only one wedge is mozzarella. Waldo bought two wedges of cheddar, and Basil also bought cheddar, but twice as much by weight as Waldo. How much does the mozzarella wedge weigh?

(b)(3)-P.L. 86-36

[redacted]

Answer:

Waldo must have bought at least 31 pounds of cheese, so Basil must have bought three wedges, since the two heaviest wedges together only total 51 pounds. Since Basil bought twice what Waldo bought, the total amount of cheese bought by the two together equals three times that purchased by Waldo alone. Now, the total weight of all the wedges at the grocery divided by 3 leaves a remainder of two, so the mozzarella wedge must leave a remainder of 2 when divided by 3. But the only such wedge is the 20 pound wedge, thus the mozzarella wedge must have weighed 20 pounds.

Correct answers were received by [redacted] (b)(3)-P.L. 86-36

Puzzle 2: Island Quandary

Waldo mentioned the problem they had getting to the Cucumberland fair recently (see last month's puzzle), and Mortimer recalled a similar occurrence from his days as a boy. It seems that three couples staying on an island wanted to cross the water using a boat that could only hold two people at a time. In those days, it was considered improper for a woman to be with a man who was not her husband unless her husband was also present. How many trips were required? Each way counts as one trip.

Answer:

It can be done in 11 trips. Let W_i and H_i be husband and wife, then on such scheme is (there are several others):

W_1 and W_2; W_1; W_1 and W_3; W_1; H_2 and H_3; W_2 and H_2; H_1 and H_2; W_3; W_2 and W_3; W_2; W_1 and W_2;

If you assume it is ok for a man to drop his wife off with another woman, even if that woman's husband is not present (this was not the intention of the puzzle), then you can do it in 9 trips:

M_1 and W_1; M_1; M_2 and W_2; M_2; M_3 and W_3; M_3; M_1 and M_2; W_3; M_3 and W_3;

Correct answers were received by [redacted] (b)(3)-P.L. 86-36

8. (U) EDITORIAL CORNER

(b)(3)-P.L. 86-36

[redacted]

REMINDER: Submissions for the July issue are due by June 26th.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

(~~FOUO~~) EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

(b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2, DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR" DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

(b)(3)-P.L. 86-36

[redacted]

Doc ID: 6823808

SECRET//COMINT

(C) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:20
(U)PE EXTERNAL PAGE

THE CLASSIFICATION OF THIS NEWSLETTER IS SECRET-HVCCO

****
* TALES OF THE KRYPT *
****
July 1996

//
****

(TSCO) TABLE OF CONTENTS:

1. (U) CA Perspective

2. (U) Calendar of Events

3. (U) CACP News

4. (U) KRYPTOS News

5. (U) Technical Health

6. (U) Puzzles

7. (U) Editorial Corner

(b)(3)-P.L. 86-36

//

1. (S) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature Richard Walton, Head of H Division, GCHQ.

~~~~~~

(S-CCO) The very last thing I did before starting to write this article was to prepare a brief presentation on cryptanalysis for a ministerial visit to GCHQ. The theme of that presentation is the essential key ingredients for maintaining a successful UK cryptanalytic capability. It should come as no surprise to any reader of this publication that high on the list is a strong and healthy partnership with Z group, NSA. From a perspective of over 50 years of close cooperation it is difficult for us to appreciate the immense courage and foresight of our forebears when they took the unprecedented leap that resulted in total pooling of the efforts in the most secret art of cryptanalysis by two great and powerful independent nations. Even under the imperatives of World War this action was unparalleled and incomprehensible in terms of the accepted norms. The continuation and flourishing of this wartime arrangement into peacetime through the UKUSA agreement is an even more incredible achievement. The result has been a unique relationship that fuelled the growth of cryptologic science and has been the main cause of the enormous success of cryptanalysis for both our countries. The relationship has also been a significant, though hidden, backdrop to the strong ties of friendship

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704
~~~~~~

that have existed between our two nations throughout post-war history.

~~(S-CCO)~~ A striking result of our post-war cooperation has been the development of modern cryptanalytic science. The popular image of cryptanalysis as a black art carried out by a set of rather odd but extremely gifted amateurs could not be further from the truth. The modern inheritors of the dilettante tradition are the academic cryptographers exemplified by Whitfield Diffie or Gus Symmonds. These amateurs work in a vacuum outside the reality of real intercept and the practical constraints of the need to provide a timely decryption service to meet actual intelligence requirements. In contrast the crypt communities at NSA, GCHQ and the other second parties constitute a fully professional force with a serious body of scientific literature. All of us can be proud to be members of that profession and heirs of the traditions forged in our shared experience in world war and its aftermath.

~~(S-CCO)~~ That well-worn Chinese line about living in interesting times has always been a part of post-war cryptanalysis. [redacted] past we have found that SIGINT in general and cryptanalysis in particular has won through against the various tides that threatened to engulf us. However, this has not been by accident or good fortune but by persistent attack by our well-motivated professionals who have seen their national duty in terms of protecting our most vital secret capabilities and preserving them for use in times of true national emergency. I hope that we in our turn can find it in ourselves to meet today's challenges as robustly as our predecessors met theirs.

~~(S-CCO)~~ Nowadays cryptanalytic skills are needed for application in other parts of the SIGINT business. To meet these needs both Z Group and H Division have expanded their range of activities beyond traditional cryptanalysis. One highly visible example is the expansion [redacted] This work offers exciting possibilities for the future but nevertheless it is important that we should not become so carried away with those possibilities that we neglect the protection of regular cryptanalysis. [redacted]. If we remember these truths and go forward together in the spirit of the founders of UKUSA, we will continue to provide our respective governments with the capability to retain the competitive edge over the rest of the world during the information age. Alone I believe that either one of us would fail. I am confident that we can live up to the standards set by our predecessors and continue to share their vision and show the courage to follow in their footsteps and so look forward to the next 50 years being as fruitful as the last.

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

****
//////////

2. (U) CALENDAR

(b)(3)-P.L. 86-36

[redacted]

July 31 KRYPTOS Literature Contest Deadline

PLAN AHEAD

Sep 17 KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)

Oct 7-11 TOOLFEST '96 (POC: [redacted] Chairperson)

Nov 19 KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)

Nov 18-22 CONSCRYPT '96, at DSD

****
//////////

3. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

[redacted] (b)(3)-P.L. 86-36

a. (U) New Faces

~~(FOUO)~~ Two new cross-trainees will begin their training in CA in July:

- [redacted] comes from a data flow position in A group, and has had prior CA experience.
- [redacted] is a former Russian linguist currently working at the NCS.

We welcome them both to the career field.

****

b. (U) Congratulations Due

~~(FOUO)~~ Congratulations are in order for two interns who were promoted this month: [redacted]

****

c. (U) New Cryptolinguist Professionalization Criteria

~~(FOUO)~~ The Language Career Panel now offers a professionalization in cryptolinguistics. If you are interested in finding out about this opportunity, please contact h114@nsa.

****
//////////

4. (U) KRYPTOS NEWS

a. ~~(FOUO)~~ Norman Roberts Award Nominations Due

~~(FOUO)~~ In recognition of Norman Roberts' talent for nurturing the skills of junior analysts, the KRYPTOS Society established the Norman Roberts Award, presented annually to a junior cryptanalyst, at NSA or GCHQ, who has made an outstanding cryptanalytic contribution. Norman had joined GCHQ in 1975 and won the respect and admiration of his colleagues for his innovative ideas and particularly for his ability to train and inspire younger analysts up to his untimely death in 1990.

[redacted] (b)(3)-P.L. 86-36

~~(FOUO)~~ Any KRYPTOS member may nominate any NSA or GCHQ employee who has approximately five years' service as of 31 July 1996, and who has made an outstanding contribution to cryptanalysis or a related discipline. (For a nominee with more than five years of CA experience, the citation should explicitly draw the judges' attention to that fact, and explain why the nomination should be considered as falling within the overarching purpose of the Roberts Award.) The nominee does not have to be a KRYPTOS member. The nomination must include the names of the proposer and the nominee, together with an account of the work which attracted the nomination. It may be classified up to TSC. Nominations are due by 30 August, and should be mailed to the KRYPTOS Society secretary, [redacted]

****

b. (U) Literature Contest Deadline Extended

~~(FOUO)~~ To ensure that judges and authors on both sides of the Atlantic have enough time to submit and evaluate papers, we have extended the deadline for submission to July 31st. Papers still have to have been written between 1 July 1995 and 30 June 1996.

****

c. (U) KRYPTOS Home Page Created for NSA Web (b)(3)-P.L. 86-36

~~(FOUO)~~ Thanks to the hard work of [redacted], there is now a KRYPTOS Home Page on the Web! To access it use the following URL

[redacted]

---

* To reach a URL directly, do the following:

- Select the "open" button (Top of the page in Netscape, bottom of the page in Mosaic). An "Open location" window will appear.
- type the URL in the space provided
- select the "open button" in the "Open location" window

You'll be taken directly to the location you typed in.

For even faster connections, do the following:

- display the email message or file that contains the URL address
- open Netscape or Mosaic
- Select the "open" button in Netscape or Mosaic.
- using the left mouse button, highlight the desired URL in the email or file
- move your cursor to the space in the "Open location" window for entering URL's
- press the middle button on your mouse. The URL you highlighted in the email should be copied to the the entry space in the "Open location" window..
- select the "open button" in the "Open location" window.

****

d. (U) Volunteers Wanted (b)(3)-P.L. 86-36

~~(FOUO)~~ [redacted] is the Chairperson for the Annual Fall Awards Banquet,

[redacted]

and she would be happy to have some additional helpers on her committee. If you are interested, please give her a call on [redacted]

5. (U) TECHNICAL HEALTH

DT Research and Advanced Technology Program.(U) [redacted] (b)(3)-P.L. 86-36
(Submitted by [redacted])

~~(FOUO)~~ The DO THAB is seeking an active role for Technical Track participants in the identification, development, and sponsorship of projects and initiatives that merit funding by the Research and Advanced Technology program in DT. This program annually identifies a fund allocation to support DO projects that are deemed compatible with the goals and ideals of the R&AT program. We are calling for help to identify and surface projects, not to spend money.

~~(FOUO)~~ This is an opportunity to become involved in developing and implementing solutions. It is an area where technical track participants can put their expertise to work in defining future systems and processes that will impact their career field. For each of the technical track skill areas, we are forming a panel that will survey its respective field and develop proposals that will compete for available funds. The skill field reps to the THAB serve as a Technology Requirements Review Panel, a subcommittee to accumulate ideas, assist with proposal development, and advance the completed proposal. We believe there are projects and ideas in all corners of the directorate that deserve attention and the chance to compete for funding. The process we seek to implement will allow the best to surface and survive.

~~(FOUO)~~ In short, we would like volunteers from the Technical Track membership to lead and participate in, a network of contacts that ferret out and surface projects that can compete for funding. We would like to establish these networks along career field lines. However, this is simply a mechanism to try to cover all bases. It is not meant to discourage cross-discipline projects from emerging. This is a community service opportunity for the entire membership. Please contact your skill field rep if you would like to participate or if you have a project proposal.

Chair
Collection
Computer Science
Cryptanalysis
Engineering and Physical Sciences
Intelligence Analysis
Language
Mathematics
Signals Analysis

[redacted]

6. PUZZLES AND PROBLEMS

[redacted] (b)(3)-P.L. 86-36

(U) July puzzles: Send answers to either or both puzzles to

[redacted]

[redacted]

Puzzle #1: Guess the Gambler

The three of us made some bets:

First, Waldo won from Molly as much as Waldo had originally.
Next, Molly won from Spike as much as Molly then had left.
Finally, Spike won from Waldo as much as Spike then had left.
We ended up having equal amounts of money.
I started with 50 cents.

Who am I?

****

Puzzle #2: Perplexing Product

Given that I*CRYPT = ZZZZZZ and that each letter stands for a different digit, what's Z?

****

Solutions to last month's puzzles:

Puzzle #1: Easy Sum

Consider the sum:

ABC + DEF + GHI = JJJ

If different letters represent different digits, and there are no leading zeros, what does J represent? (Note, the question only asks for J - there may be several possibilities for the other letters.)

Solution:

Since there are no leading zeros, J must be 7, 8, or 9, since JJJ = ABC + DEF + GHI >= 100+240+350 = 690. Now, the remainder left after dividing any number by 9 is the same as the remainder left after dividing the sum of the digits of this number by 9. Next note that 0+1+2+3+4+5+6+7+8+9 has a remainder of 0 after dividing by 9, and since JJJ has a remainder of 0, 3, or 6, it follows that J must be 9, since it's the only number from 7, 8, and 9 that leaves a remainder of 0, 3, or 6 if you remove it from the sum 0+1+2+3+4+5+6+7+8+9.

Nigel Hodges provided the following analysis to find the number of solutions that the letters A through I have:

999 = 157 + 462 + 380 for example

JJJ = ABC + DEF + GHI

To get the full list of solutions, first note that we can interchange A, D and G without affecting the sum. Also B, E and H. Also C, F and I.

Since the sum of the digits on the LHS is 27 and on the RHS is 36, we need one carry of 1.
So we need to solve either

(b)(3)-P.L. 86-36

C+F+I=9, B+E+H=19, A+D+G=8

or

C+F+I=19, B+E+H=8, A+D+G=9

So, solving one set immediately solves the other.

Take C+F+I=9, B+E+H=19, A+D+G=8

{A,D,G} = {7,1,0} {6,2,0} {5,3,0} {5,2,1} {{4,3,1}

It turns out that, for each of these, there is a unique solution for {C,F,I}. Obviously this then leaves a unique solution for {B,E,H}:

```
{A,D,G} = {7,1,0} {6,2,0} {5,3,0} {5,2,1} {4,3,1}
{B,E,H} = {8,6,5} {8,7,4} {8,7,4} {8,7,4} {8,6,5}
{C,F,I} = {4,3,2} {5,3,1} {6,2,1} {6,3,0} {7,2,0}
```

Each vertical block of solutions yields 216 solutions so there are 1080 altogether.

```
{A,D,G} = {4,3,2} {5,3,1} {6,2,1} {6,3,0} {7,2,0}
{B,E,H} = {7,1,0} {6,2,0} {5,3,0} {5,2,1} {4,3,1}
{C,F,I} = {8,6,5} {8,7,4} {8,7,4} {8,7,4} {8,6,5}
```

This generates 1080 further solutions making 2160 in total.

The solutions form 360 families of 6 each e.g.

```
999 = 157 + 462 + 380
    = 157 + 380 + 462
    = 462 + 157 + 380
    = 462 + 380 + 157
    = 380 + 157 + 462
    = 380 + 462 + 157
```

Answers were received from [redacted]

[redacted]

Puzzle 2: Hard Sum

No instructions. When you get the right answer, you'll know it.

```
HARD + HOKY = LOLY
HOKY + CIA = PYKYL
```

Solution:

Just a little bit of lateral thinking required:

```
FOUR + FIVE = NINE
FIVE + TWO = SEVEN
```

(b)(3)-P.L. 86-36

Answers were received from [redacted]

[redacted]

//
##

7. (U) EDITORIAL CORNER

REMINDER: Submissions for the August issue are due by July 26th.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

(b)(3)-P.L. 86-36

\\\

THE CLASSIFICATION OF THIS NEWSLETTER IS ~~SECRET HVCCO~~

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

[redacted]

(b)(3)-P.L. 86-36

[redacted]

SECRET//COMINT

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:19
(U)PE EXTERNAL PAGE

(b)(3)-P.L. 86-36

****
* TALES OF THE KRYPT *
****
August 1996

//
****

(FOUO) TABLE OF CONTENTS:

1. (U) CA Perspective
2. (U) Calendar of Events
3. (U) CACP News
4. (U) KRYPTOS News
5. (U) Technical Health
6. (U) Community Service
7. (U) Puzzles
8. (U) Editorial Corner

(b)(3)-P.L. 86-36

//

1. (S) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature [redacted] the deputy chief [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~~~~~

(FOUO) You say you're a Z professional, eh? Been here since Z was formed. Love it here. Want to keep doing what you're doing, getting better and better. Dedicated to furthering the CA mission of the finest Agency on the face of the Earth. Good for you! Z needs more people just like you. Now, here's my advice to you: Leave. Get out. Keep us in your heart, but go away for awhile.

(FOUO) [To make this paper easier for me to write, I've approached it as one Z person writing to another. It applies equally well to people in any organization.] Given this opportunity to speak my mind on a subject of my choosing, I thought I would share my views on diversification as an ingredient of a healthy career growth pattern. The diversification I'm talking about means more than getting a ticket punched or satisfying requirements for professionalization or tech track membership. Diversification means learning to thrive in a variety of changing environments, and in today's world, that's a key to personal growth and professional success.

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted] (b)(3)-P.L. 86-36 9/23/2010
~~~~~~

(FOUO) Diversification cannot be had by going to another organization under a temporary arrangement. The benefits kick in only when you become a member of a new organization that has culture, values, goals and resources substantially different than the one you call home. Until you depend on another organization for your performance appraisal and your career advancement, you haven't made the sort of commitment that true diversification requires. A detail to another NSA organization is an easy way to expand your knowledge of other technologies and other missions. But it isn't what I mean when I use the term diversification. Let me use some examples to explain why I think diversity is worth the effort: Fluency of Thought - When our family moved to Germany in 1986, our daughter [redacted] was three years old. By the time we decided to return to the U.S. four years later, she was fluent in German, having attended nursery school, kindergarten, and two years of public school in classrooms where she was the only American. My wife and I asked a teacher at the base school -- who had taught and raised children on three continents -- how we might help [redacted] keep up her German after we returned to the States. "Don't worry about whether [redacted] will be able to speak German ten or fifteen years >from now," he said. "She'll remember for the rest of her life that there are at least two ways of expressing every thought that comes into her head. That's the real benefit of being bilingual early in life."

(b) (6)

(FOUO) Just as linguistic diversity has a permanent effect on a child's thought processes, career path diversity can permanently improve a person's ability to see issues from several different viewpoints simultaneously. That's a very valuable ability, whether you're a researcher, an analyst, an engineer or a manager. (By the way, [redacted] cried every day for the first month of German nursery school. Now she's flown back to Bad Aibling by herself every summer since she was eight, she still speaks German like a native, and her friends and experiences in Bad Aibling are her greatest treasures.)

(S-CCO) Breadth of Experience - Let me get even more personal. I don't particularly like change, and I tend to try to minimize change in my personal life. And I don't mean to suggest that anyone needs to make as many career-path turns as I've made -- Counting Cryptomath and SCEDP tours, I've been in nineteen different offices since I came to NSA. But I think my own career demonstrates the value of diversification to an individual and to an organization. In 1981 I left a rewarding job in G43 to take a tour in NSOC. That job led to a position in G7, after which I managed the [redacted] relevant to the Z3 mission. And in the past two weeks I've found that several of my recent assignments are directly related to my new job. I'm able to do lots of things not because I'm particularly brilliant, but because I've done lots of things. Adaptability - Change is getting lots of attention nowadays because of the unprecedented rate at which factors that influence our personal and professional lives are changing. Whether or not you enjoy change is irrelevant: You like it or you don't. Trying to avoid change by staying put for as long as possible is futile: Your environment will change continuously, and the

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

[redacted]

better you cope with change, the more satisfied and productive you will be. The issue is whether you are able to use change to your advantage, to see change as an agent for personal and professional growth. If you are, you will learn to find opportunities to expand your technical and organizational base. You will take some risks, but you will grow accustomed to that, and you may come to relish it.

(U) Network - One of the collateral benefits of a curvaceous career path is the enlargement of one's network. Having a good network is crucial to your ability to make things happen, and making things happen is what most of us are paid to do. Your network is simply the people whom you know and trust, who do not report to you, upon whom you rely for getting things done. The more places you've been, the larger and more effective your network can be.

(U) A career path like mine is not for everyone, and I have to confess that when I came to Z3 last year, after fourteen years away from cryptanalysis, it felt like coming home at last. There's certainly nothing wrong with thinking of yourself as a Z-Grouper, no matter where you go or how long you stay away. But for your own good and for the good of the organization, if you haven't taken a permanent assignment outside Z for awhile, you should seriously consider doing so.

****
//////////

2. (U) CALENDAR

PLAN AHEAD

Sep 17	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)
Oct 7-11	TOOLFEST '96 (POC: [redacted] Chairperson)
Oct 17	KRYPTOS Annual Luncheon
Oct 28-30	C2C Conference
Nov 12-14	Cryptanalytic Computing Conference at CCS
Nov 19	KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)
Nov 18-22	CONSCRYPT '96, at DSD

(b)(3)-P.L. 86-36

****
//////////

3. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

a. (U) New Certification Requirements

~~(FOUO)~~ The requirements for professionalization as a Cryptanalyst have been revised and are currently available from the CA Career Panel office. The new criteria offer a specialization in one of four areas: Mathematics, Engineering, Computer Science, or Conventional CA. Additionally, the Language Career Panel has just released guidelines for certification as a Cryptolinguist. If you would like additional

(b)(3)-P.L. 86-36

[redacted]

information about either of these certifications, please contact the CA Career Panel office (h111@nsa) on [redacted] for CA professionalization, or the Language Career Panel office [redacted] on [redacted] for Cryptolinguistics.

****

b. (U) Tutors Wanted - Calling all Senior Cryptanalysts (b)(3)-P.L. 86-36

(FOUO) The Cryptanalysis Career Panel is looking for professionalized cryptanalysts willing to work with aspirants for CA certification in a one-on-one situation in preparation for the annual CA PQE held in May. The details of the arrangements are to be worked out between the aspirant and the tutor. If you are interested in becoming a PQE tutor or want more information, please contact the CA Career Panel office at h111@nsa or on 963-4596(s).

****

c. (U) CACP LOGO SOUGHT

(U) The CA Career Panel is holding a contest during the month of August to design a logo for the panel which will be used on the Peter Jenks Award plaque, as well as for other things in the future. Please submit your design(s) to the panel office in OPS 2B room 3036D. The winner will receive an ice cream sundae.

****
//

4. (U) KRYPTOS NEWS

a. (FOUO) Call for Peter Jenks Award

(FOUO) This award, jointly offered by KRYPTOS and the CACP, may be granted yearly to an individual in recognition of exceptional service and contribution to the CA community. This may reflect work spanning an individual's entire career, or be reflective of current and/or unique contributions. Potential award recipients include NSA/CSS civilian employees and military assignees who are active in the CA community.

(FOUO) The President of the KRYPTOS Council and the Chairman of the Cryptanalysis Career Panel are responsible for providing the guidelines for recommending individuals for this award. The following basic selection criteria also apply:

- The service and contribution must be in the field of cryptanalysis and reflect efforts which exceed those expected in the performance on the job.
- Such endeavors may include, but are not limited to, serving on the CACP, as a KRYPTOS officer, as a member of a CA TTRP, as a judge for an award or contest, or designing and teaching a new CA course, coordinating technical talks, or other efforts which serve the cryptanalysis community as a whole.

(FOUO) Any individual, or group of individuals, may nominate/recommend someone for this Award. Such nominations, detailing the contributions the individual has made to the CA community, should be forwarded to the Secretary of the KRYPTOS Council, [redacted] by 13 September. (b)(3)-P.L. 86-36

[redacted]

~~(FOUO)~~ The President of the KRYPTOS Council and the Chairman of the Cryptanalysis Career Panel will be the primary selection officials. They may, at their discretion, add representatives from either the Council or the Career Panel, to assist them in their deliberations.

~~(FOUO)~~ This award may be given annually, but there may be one or more years in which the award is not given. A Certificate of Honorable Mention may also be awarded, at the discretion of the Council. Such awards will be made at the Annual KRYPTOS luncheon.

5. (U) TECHNICAL HEALTH

a. ~~(FOUO)~~ Update on Z Boards

~~(FOUO)~~ Since there have been some changes recently in the Boards in Z which deal with technical health issues, we are providing the following:

1. Z Technical Career Advisory Board

Plan Director - [redacted] (replacing Floyd Weakley)
At-Large Member - [redacted] (replacing [redacted]
Skill Field Representatives:
CA - [redacted]
Math - [redacted]
Signals Analysis [redacted]
Computer Systems
Collection/IA -
Engineering - [redacted]
Executive - [redacted]
Z Training Coordinator - [redacted]

(b)(3)-P.L. 86-36

2. Office Technical Health Board (OTHB) Chairs

[redacted]

6. (U) COMMUNITY SERVICE

(b)(3)-P.L. 86-36

a. ~~(FOUO)~~ Floyd Weakley Honored

~~(FOUO)~~ During this past month, Floyd Weakley, Z5 Special Assistant, was selected to receive the prestigious Roy Wilkins Renown Service Award conferred by the NAACP. The award, for exemplary service in support of the goals of the NAACP, recognized Floyd's contributions

[redacted]

during his career at NSA. Needless to say, there was stiff competition for this award, but Floyd's tireless and continuous efforts in support of the diversity goals of the NAACP obviously impressed the selection panel. The award was presented to Floyd at a special banquet as part of the NAACP's National Convention in Charlotte, NC.

~~(FOUO)~~ Also, at the Excellence in Federal Career Awards Program held in early May, Floyd was selected as the Gold Medal Winner, from among all the nominees from Federal Agencies across Maryland, for the Equal Employment Opportunity Service Award. Floyd was recognized in particular for his role in the hiring of mathematicians by this Agency. He was lauded for his staunch support of a number of outreach programs specifically aimed at minorities and women. He was credited with helping in a new recruiting effort, aimed at minority math students, which in turn helped the Director surpass his recent minority hiring goal of 33%. That Floyd invested literally hundreds of hours of labor-intensive work over and above his normal workweeks in fulfillment of the duties and responsibilities inherent in all these and other related endeavors was also cited.

(U) Congratulations to Floyd for these well-deserved recognitions!

b. (U) NEW ARCHIVES HOME PAGE SOON TO BE UNVEILED

~~(FOUO)~~ Stay tuned for the new NSA/CSS Archives Home Page which will be available on-line soon. This Home Page will feature present and past issues of "NSA's Attic," services provided by the Archives, photos of SIGINT platforms, field sites, and personalities, and finally special accessions. Send in your suggestions as to what other areas of interest you would like to see on this page to either [redacted], or [redacted]. We can also be reached by e-mail at [redacted] or [redacted]

8. (U) PUZZLES

a. (U) August Puzzle #1: Waldo Phone Home: (b)(3)-P.L. 86-36

Waldo is a bit absent minded, and the only way he can remember his own phone number is that if you divide it by its reverse, you get an integer greater than one. What's Waldo's phone number?

b. (U) August Puzzle #2: Rameses' Pyramid

Rameses wishes to build a great pyramid for his interment. The structure will have a square base and be solidly composed of cubical stone blocks. Each level of the pyramid contains one less block per side as the pyramid rises. Rameses has available an initial work force of 35,000 slaves. Each morning the available labor pool is divided into crews of 17 slaves each. Any remainder that cannot form a full crew get the day off but are available for work the following day. Each crew can lay one block of the pyramid each day. Unfortunately, the heat of the desert sun causes the death of one member of each crew each day. Work ceases on the project when it can be determined that there will be insufficient slaves available to raise the pyramid one more level. (The Egyptians have

precalculated how many levels they will need so the top level has only one block.) Each stone block measures 3 meters per side.

How many days will it take to construct Rameses' pyramid? How tall will it be? How many of the original slaves survive the construction? How many total blocks make up the pyramid?

---

c. (U) Answers to July puzzles:

Puzzle #1: Guess the Gambler

The three of us made some bets:

First, Waldo won from Molly as much as Waldo had originally.
Next, Molly won from Spike as much as Molly then had left.
Finally, Spike won from Waldo as much as Spike then had left.
We ended up having equal amounts of money.
I started with 50 cents.

Who am I?
Solution:

Let Waldo start with w, Molly with m, and Spike with s cents. Following the above account we get the following progression of monies:

W = 2*w, M = m-w
M = 2*(m-w), S = s-(m-w) = s+w-m
S = 2*(s+w-m), W = 2*w-(s+w-m) = w+m-s

And so Waldo finished with w=m-s, Molly with 2*(m-w), and Spike with 2*(s+w-m). Since these must all be equal, we have three equations with three unknowns, so solve. This gives us that 4*m = 5*s and 3*s = 4*w. Now, if s = 50, this implies that w = 37.5 which is impossible since the number of cents must be an integer. If w = 50, then s = 66.666..., again impossible. Finally, if m = 50, then s = 40, and w = 30 cents, which works. It follows that I am Molly.

(FOUO) Answers were received from [redacted] (b)(3)-P.L. 86-36

Puzzle #2: Perplexing Product

Given that I*CRYPT = ZZZZZZ and that each letter stands for a different digit, what's Z?

Solution:

This is easy enough to do by brute force, but it is possible to reduce the number of choices one must try:
ZZZZZZ = Z*111111 = Z*3*7*11*13*37, and so I must be either 3 or 7. But if I = 3, then CRYPT = Z*37037, giving (b)(3)-P.L. 86-36

[redacted]

CRYPT = 37037 if Z = 1, or CRYPT = 74074 if Z = 2. Either one is a contradiction. Thus, I = 7, and so CRYPT = Z*15873. Since each letter must stand for a different digit, a quick check with a calculator gives that the only answer is Z = 6.

Answers were received from [redacted] (b)(3)-P.L. 86-36

[redacted]

//
##

9. (U) EDITORIAL CORNER

REMINDER: Submissions for the September issue are due by August 26th.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted] (b)(3)-P.L. 86-36

[redacted]

\\\

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2, DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR" DATE OF SOURCE: 3 SEP 1991

[redacted]

[redacted]

SECRET//COMINT
(b)(3)-P.L. 86-36

(S) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:21
(U)PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
September 1996

//
****

~~(FOUO)~~ TABLE OF CONTENTS:

1. (U) CA Perspective
2. (U) Calendar of Events
3. (U) CACP News
4. (U) KRYPTOS News
5. (U) Technical Health
6. (U) Community Service
7. (U) Puzzles
8. (U) Editorial Corner

(b)(3)-P.L. 86-36

//

1. ~~(S)~~ PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature [redacted] at CCR.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted] (b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

2. (U) CALENDAR

Sep 12 S & E Talk

(b)(3)-P.L. 86-36

[redacted]

Sep 12 INFOSEC DAY

Sep 17 KRYPTOS Talk, [redacted], "Pattern Analysis of Clay Scratchings: The Decipherment of Linear B" (Friedman, 1300)

PLAN AHEAD

Oct 7 Briefing on Data Network Threat (see below)

Oct 7-11 TOOLFEST '96 (POC: [redacted] Chairperson)

Oct 15-22 Nov - MINISCAMP (see below)

Oct 17 KRYPTOS Annual Luncheon

Oct 17 FUTURES DAY

Oct 28-30 C2C Conference

Nov 12-14 Cryptanalytic Computing Conference at CCS

Nov 19 KRYPTOS Talk (Subject/Speaker to be Announced) (Friedman, 1300)

Nov 18-22 CONSCRYPT '96, at DSD

[redacted] (b)(3)-P.L. 86-36

****
//////////

3. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

a. (U) New Training Document Available

~~(FOUO)~~ The CACP document "Training as a Certification Requirement" is complete and will be available by email from the CACP. Thanks to the able skills of our home page updater, the document is also available through Mosaic. You can access it from the M82 Organizational Page (H111 - Career Panels), then under Professionalization Information. This document outlines the NCS courses needed for professionalization as a cryptanalyst under the new requirements.

URL is [redacted]

****

b. ~~(FOUO)~~ CA Intern/Cross Trainee promotions and awards for August:

[redacted]

Promotion
Promotion

SPCA
SPCA
SPCA
SPCA

[redacted] (b)(3)-P.L. 86-36

****

[redacted]

c. (FOUO) GOLD BUG Award Announced

(FOUO) At a recent meeting of the Cryptanalysis Career Panel it was announced that the Director has approved a GOLD BUG award for [redacted] amazing diagnostic work [redacted]

CONGRATULATIONS CHRISTINA!!!!

(b)(3)-P.L. 86-36

4. (U) KRYPTOS NEWS

a. September Talk Announced -

(U) In 1900 Sir Arthur Evans unearthed clay tablets in an unknown writing system which he named Linear B. For over 50 years all attempts to decipher this system failed. The puzzle was finally cracked in 1952 by a British architect named Michael Ventris. His method was based on that of the American scholar Alice Kober. Of all the decipherments of ancient scripts, the decipherment of Linear B is generally considered to be the most technically elegant. The technique involved recognizing patterns in the written signs and interpreting these patterns as grammatical constructs. No assumption of the underlying language was made until the last stage of the decipherment. Come hear [redacted] discuss how pattern analysis led to this decipherment.

b. (FOUO) LAST CALLS

(FOUO) REMINDER - ALL NOMINATIONS for the PETER JENKS AWARD and the NORMAN ROBERTS AWARD are due by 13 September. Please send via e-mail to [redacted]

5. (U) Technical Health

(b)(3)-P.L. 86-36

a. (FOUO) Chief Z Announces INFOSEC DAY

(TSC) I am pleased to announce Z Group's INFOSEC Day, which will be held on Thursday, on Thursday, September 12, 1996 in the Friedman Auditorium. This day of briefings is based on IN-700, the National Information Systems Security course, and contains several interesting presentations which will help to familiarize Z Group personnel with INFOSEC issues. We are fortunate to have speakers who are experts in their topics and who are looking forward to the opportunity to share the INFOSEC world with Z Group.

(TSC) From my personal experience I can site many examples of where my knowledge of INFOSEC issues and technology was critically important to assessing current and future COMINT needs. I can also say that I am [redacted] and every one of us carry the responsibility of ensuring that U.S. and

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

DoD national security is maintained.

(TSC) I urge you to attend this day of worthwhile presentations. Seating will be on a first come, first served basis. Any questions you may have can be directed to [redacted] the Z Training Authority, who is coordinating the day's presentations.

[redacted] Chief Z

(b)(3)-P.L. 86-36

INFOSEC DAY - 12 September 1996
Friedman Auditorium

8:30 - 9:30	INFOSEC Overview
9:30 - 10:30	Information Warfare
10:45 - 11:45	Multi-Level Information Systems Security Initiative (MISSI)
LUNCH	
1:15 - 2:30	History of COMSEC Monitoring
2:30 - 3:45	Vulnerabilities in Operational Automated Information Systems

[redacted]

b. (FOUO) MINISCAMP

(TSC) The Fall 96 MiniSCAMP will be held Oct. 15 - Nov. 22 at IDA-CCS in Bowie on diagnosis and exploitation of speech and video compression. (Note the change in venue.) For further technical information, visit the Mosaic (Webworld) web page at

[redacted]

(FOUO) If you are interested in participating, please get your supervisor's approval to participate full time for the 6 weeks. Then contact a member of the MiniSCAMP Committee representative Nominees will be notified of their selection by mid-Sept.

[redacted]
Fall 96 MiniSCAMP p.o.c.

(b)(3)-P.L. 86-36

[redacted]

c. (FOUO) Briefing on Data Network Threat Scheduled

[redacted]

~~(C-CCO)~~ Mr. Bill Black, Head of the Information Warfare Center, will be briefing Z Group personnel on the Data Network threat. Mr. Black is a dynamic speaker and his briefing on this high interest SIGINT challenge has received great accolades throughout the Intelligence Community.

(U) The briefing is scheduled for Monday, 7 October 1996 from 1315-1515 in the Friedman Auditorium. The briefing lasts one hour. The remaining time will be used for questions.

(U) This briefing is US ONLY and will be videotaped.

****

6. (U) Community Service

a. (U) Speaker Announced for S and E Luncheon

(U) On Friday October 25 1996 the Society will have a special luncheon. The guest speaker will be [redacted] Commander of Apollo 13, as in "Houston we have a problem" speaking on "Apollo 13 a Successful Failure" (one of the last lines of the movie). (b) (6)

When: Friday 25 October 1996
Where Canine Suite Ops 2B
Time 11:00
Cost TBD (probably around $8 for members)

Tickets will go on sale on a date TBD. Members will have first crack at them.

****
//

7. (U) PUZZLES

a. ~~(FOUO)~~ Solutions to August puzzles:

~~(FOUO)~~ Both puzzles could have been solved by computer programs, but analytical solutions are provided here for those that are interested:

Puzzle #1: Waldo Phone Home:

Waldo is a bit absent minded, and the only way he can remember his own phone number is that if you divide it by its reverse, you get an integer greater than one. What's Waldo's phone number?

Solution:

If you allow trailing 0s, there are many trivial answers, so let's assume Waldo doesn't allow such niceties. In that case, still either 879-9912 or 989-9901 works, so either Waldo is not as absent-minded as he claims, or let's hope he never has to phone home.

[redacted] offered the following solution to the problem:

We have k*(a*10^6 + b*10^5 + ... + g). = (g*10^6 + f*10^5 + ... + a)

so immediately, 1) k*a<10 (since the product is 7 digits) (b) (3)-P.L. 86-36

[redacted]

2) k*g = a mod 10
3) k*a <= g

so we can examine the k's.

k=9: Rule 1 says a=1 is the only possibility, which makes g=9 (rule 2). so we have 9*1bcdef9 = 9fedcb1. Mod 100, we have 90f+81 = 10b+1, or 90f+80=10b. We cannot have a carry from the 9*b multiplication, so b=1, f=7 and b=0, f=8 are the only choices. But for b=1, we cannot have any carries from 9*c, so f=9 - a contradiction. So we have 9*10cde89 = 98edc01. The 9*c product must now create a carry of 8, so that c = 8 or 9. Computing mod 1000, we have 900e+801 = 100c+1, giving c=8,e=0 and c=9,e=9 as choices. For c=8, only d=9 produces the required carry of 8 (i.e. 9*89 = 801), but 9*1089089 = 9801801. For c=9, e=9, d>=8, and in fact we find for d=9, 9*1099989 = 9899901.

k=8: a=1 is again the only choice, but there are no solutions to 8*g=1 mod 10.

k=7: a=1 forces g=3, but rule 3 is immediately violated.

k=6 and k=5: see k=8.

k=4: a=1 is incompatible with rule 2. For a=2, g=3 or 8 are possible, but g=3 violates rule 3. With g=8, we can have no carries from 9*b, so b=0,1,2 are possible. Mod 100, 40f+32 = 10b+2, which has no solutions for b=0 or 2, and gives f=2 or f=7 for b=1. By analogy to rule 3, however, 4*b<=f, and so f=7 is the only choice, giving 4*21cde78 = 87edc12. This requires a carry of 3 from the 4*c product, leaving only c>=7. Mod 1000, we have 400e+312 = 100c+12. c=8 has no solutions, leaving c=7,e=1 or e=6 and c=9,e=4 or e=9. Since 4*219=876, both c=9, e=4 and c=7, e=6 are eliminated. For c=7 and e=1, d=8 and d=9 the only possibilities, and both fail. So we are left with c=9,e=9, and a quick check reveals that 4*2199978 = 8799912.

k=3: a=3 requires g=3, but rule 3 is violated. This also occurs for a=2, g=4. For a=1, we get g=7 and 3*1bcdef7 = 7fedcb1. This requires a carry of 4 from the 3*b product, which is impossible.

k=2: a=4 allows g=2 or 7, but both break rule 3. There are no solutions to rule 2 for a=3 or 1. For a=2, g =1 or 6 are possible, but only g=6 meets rule 3, giving 2*2bcdef6 = 6fedcb2, which requires an impossible carry of 2.

k=1 is disallowed by the problem statement.

so the solutions are (2199978,8799912) and (1099989,9899901).

(b)(3)-P.L. 86-36

Solutions were received by [redacted]

[redacted]

---

c. Puzzle #2: Rameses' Pyramid

Rameses whishes to build a great pyramid for his interment. The structure will have a square base and be solidly composed of cubical stone blocks. Each level of the pyramid contains one less block per side as the pyramid rises. Rameses has available an initial

(b)(3)-P.L. 86-36

[redacted]

work force of 35,000 slaves. Each morning the available labor pool is divided into crews of 17 slaves each. Any remainder that cannot form a full crew get the day off but are available for work the following day. Each crew can lay one block of the pyramid each day. Unfortunately, the heat of the desert sun causes the death of one member of each crew each day. Work ceases on the project when it can be determined that there will be insufficient slaves available to raise the pyramid one more level. (The Egyptians have precalculated how many levels they will need so the top level has only one block.) Each stone block measures 3 meters per side.

How many days will it take to construct Rameses' pyramid? How tall will it be? How many of the original slaves survive the construction? How many total blocks make up the pyramid?

Solution:

Each block added results in the death of exactly one slave, and when there are less than 17 slaves, no more blocks may be added, so the pyramid consists of at most 35000-16 = 34984 blocks. The top level needs one block, the next 4, and in general, the i'th level from the top needs i^2 blocks, and so a pyramid n levels tall requires $1 + 2^2 + 3^2 + \ldots + n^2 = n(n+1)(2n+1)/6$ blocks. This is between $n^3/3$ and $(n+1)^3/3$, and solving $n^3/3 = 34984$, we get that the maximum number of levels is either 46 or 47, with a quick check showing that 46 is correct. It follows that the pyramid is 46*3 = 138 meters tall, consists of 33511 blocks, and the number of slaves surviving the construction is 35000-33511 = 1489.

To compute the number of days required for the construction, note that if there are m slaves on a given day, the number of blocks added is between m/17 and m/17 - 16/17, and given k days, it can be easily shown that the number of blocks added is between
$m/17 + (16/17)m/17 + \ldots + (16/17)^{(k-1)}m/17$ and
$m/17 + (16/17)m/17 + \ldots + (16/17)^{(k-1)}m/17 - k*16/17$.
Summing the geometric series, we get $m*(1-(16/17)^k)$, and so to find the number of days required, we solve $35000*(1-(16/17)^k) = 33511$, and get $(16/17)^k = .04254$ or k = 52.08. Since this came from an upper bound on the number of blocks, it's a lower bound on the number of days; thus it will take at least 53 days to build the pyramid. Checking the lower bound, we see that the number of blocks that can be added in 53 days is greater than 33542, so the pyramid can indeed be built in 53 days.

Solutions were received from [redacted]

d. ~~(FOOD)~~ September puzzles:

(b)(3)-P.L. 86-36

Send answers to any or all puzzles to [redacted]

Puzzle #0: Tom Swifty (SAID = 6)

A Tom Swifty is a phrase in which what Tom states is punningly related to how he says it; some examples:

[redacted]

"I love sugar in my coffee," Tom said sweetly.
"I'm dying," Tom croaked.

In this problem, you are to replace SAID with
a 6-letter word that makes the phrase a nice
Tom Swifty.

"Irish wood is the best," Tom SAID.

''''''

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted] (b)(3)-P.L. 86-36

\\\

Doc ID: 6823809

TOP SECRET//COMINT

(C) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:20
(U)PE EXTERNAL PAGE

(b)(3)-P.L. 86-36

****
* TALES OF THE KRYPT *
****
November 1996

//
****

CORRECTION: Please note that the KRYPTOS ballot had an error for which this editor takes full responsibility. The office for which [redacted] and [redacted] are running is SECRETARY, not TREASURER. If this affects your voting, please use the ballot attached at the end of the newsletter and resubmit it. Since the tops have not yet been removed >from those ballots already received, it is easy enough to replace an old ballot with a new one. Again, the only change is for the office in question. My apologies.

++
//

(TOUO) TABLE OF CONTENTS:

1. (U) CA Perspective

2. (U) Calendar of Events

3. (U) CACP News

4. (U) KRYPTOS News

5. (U) Technical Health

6. (U) Community Service

7. (U) Puzzles

8. (U) Editorial Corner

//

1. (C) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature [redacted]

(b)(3)-P.L. 86-36

~~~~~~

(TSC) As some of you are aware, I disappeared from Z about a year ago in order to pursue an assignment in the STDP. When I put together an STDP program saying I wanted to learn about networks and network security, it was with a good bit of naivete - because at the time I didn't know thing one about networks or how they operated. I only knew that as encryption and other security mechanisms moved into the network

Approved for Release by NSA on 09-28-2023, FOIA Case # {61704

[redacted] (b)(3)-P.L. 86-36
~~~~~~

world, we in Z needed to develop some understanding of this world in order to do the right things in the future. I chose as my assignment

[redacted]. Going there was akin to becoming a mathematical expatriate, as I joined a group which was composed of engineers and computer scientists with little background in cryptography or cryptanalysis. Did I know what I was getting into? No way. Am I glad I did it? Absolutely.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(3)-P.L. 86-36

[redacted]

(FSC) What do we have to do to be a player? Well, first and foremost it is important for us to be more in touch with what is going on outside. There are a lot of smart folks trying to solve the network security problem. The work in this area isn't appearing in mathematical journals - but a lot is available on the Internet. In fact, if I had to get on a soapbox, it would be to make the point that fast, convenient access to the Internet from our workspaces - even from our desks - is as vital to being prepared for the future as the next Cray. (Ok, ok, perhaps a little exaggeration there, but not TOO much!)

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(U) I'll soon be off to another assignment, continuing to work "outside the fold". I have a much better idea what I'm getting into this time, and I'm looking foward to it. I hope a few of you will consider joining me.

****
//////////

2. (U) CALENDAR

Nov 4 Seven Philosophies of Native American Men, [redacted] (Friedman 1000-1100)

Nov 6 Talk on Bletchley Park, by [redacted] former British Intelligence officer (Friedman 1030) (see 5b)

(b)(6)

Nov 8 IAI Talk on Information Warfare, [redacted] (Friedman 1300)

Nov 12-14 Cryptanalytic Computing Conference at CCS

Nov 19 KRYPTOS Election and Talk (Subject/Speaker to be Announced) (Friedman, 1300)

Nov 18-22 CONSCRYPT '96, at DSD

****
//////////

3. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

a. (U) Professionalization News

(FOUO) Congrats to newly certified Cryptanalyst, [redacted]

(b)(3)-P.L. 86-36

****

b. (FOUO) Membership Changes Announced

(FOUO) [redacted] is the newest member of the CACP, and [redacted] is now on the CA TTRP.

[redacted]

c. (FOUO) GOLD BUG Award Presentation

(b)(3)-P.L. 86-36

(FOUO) The Gold Bug Award ceremony was held on 9 October in the DDO conference room. At this ceremony, [redacted] Chief Z, presented the Gold Bug Award to [redacted] of R51 and the Gold Bug Team Award to [redacted] The Gold Bug is awarded by the Cryptanalysis Career Panel for an outstanding achievement in the field of cryptanalysis. This was the first time that the award was given to analysts outside of NSA, and reflects the increased emphasis on teaming across the intelligence community to solve difficult problems.

4. (U) KRYPTOS NEWS

a. KRYPTOS Luncheon a Great Success

~~(FOUO)~~ The Annual Fall Luncheon was held again this year at the Fort Meade Officers' Club, and [redacted] and her team did an excellent job organizing the event. A number of awards were announced:

Distinguished Members: [redacted] at NSA GCHQ

Norman Roberts Award: [redacted]

Peter Jenks Award: [redacted]

(b)(3)-P.L. 86-36

Literature Contest:
First place - [redacted] GCHQ
Second place -
Third place -
Honorable Mention - [redacted] GCHQ
Honorable Mention -

b. ~~(FOUO)~~ Abstracts of Winning Papers

(1) ~~(TSC)~~ [redacted]

Due to Z group policy this has been removed. We will try to make it available to the internal Z group web in the near future.
Sorry for the inconvience. Kryptos Home page Web master

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

[redacted] (b)(3)-P.L. 86-36

[redacted]

~~(FOUO)~~ My primary objective in writing the report was to document these features both for the historical record and for use if the fighting starts up again and similar systems reappear. Since, however, fewer and fewer people are exposed at all to manual crypt, it seemed a good idea to flesh out the descriptions of the systems with a brief account of how they were solved. This just might help someone faced with working such systems in the future.

[redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[redacted]

(4) ~~(TSC)~~ [redacted]

~~(TSC)~~ This paper describes two diagnostic problems and new attacks for both of them. It also provides an exact analysis of the behaviour of one of these attacks and heuristic/experimental measurements on the behaviour of the other.

[redacted]

[redacted] (b) (3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TSC)~~ It is worth mentioning that the improving results of the paper was presented as one of the problems for this year's Summer Student Programme at GCHQ, with the result that the second algorithm has now been (considerably) improved upon - although operational programs using the new methods are still under development.

(5) [redacted]

[redacted]

5. (U) Technical Health

(b)(3)-P.L. 86-36

a. ~~(FOUO)~~ Chief Z Announcement

~~(FOUO)~~ Recently [redacted] was pleased to announce that [redacted] and [redacted] have been elevated to Senior Level Expert. Both [redacted] and Tom are widely appreciated for the emphasis they have placed on the collection/signals/development/processing issues. They are also models for their mentoring and leadership activities. He asked that everyone join in congratulating the both of them.

(b)(6)

b. ~~(FOUO)~~ [redacted] TALK ON BLETCHLEY PARK

~~(FOUO)~~ The Center for Cryptologic History will present a talk by [redacted] a former British intelligence officer, on the successful efforts by analysts at Bletchley Park against Axis codes and ciphers

during World War Two. [redacted] will also discuss his work to preserve Bletchley Park as a memorial to those who served there and their extraordinary achievements. As part of his presentation, [redacted] will address the question of whether Colossus, the British cipher machine used against German traffic, was actually the world's first computer.

(FOUO) [redacted] talk will take place on 6 November at 1030 in the Friedman Auditorium. All Agency personnel are encouraged to attend this fascinating view of cryptologic history.

(FOUO) NOTE: Attendees at the morning lecture will be able to earn NCS credit for IR-220, Current Topics in Information Resources. Just be sure to fill in the requested information on the sign-in sheet that will be available in the auditorium.

(FOUO) On the afternoon of 6 November, [redacted] will conduct a seminar on Colossus. Using declassified documents, [redacted] re-created this computing device and was able to sponsor its first running in 1996.

(FOUO) If you would like to hear first hand how Colossus was built, discuss the nature of the computer, and debate its origins, join [redacted] on the 6th at 1300 in room 2C086. Space is limited for this seminar, so please contact the Center for Cryptologic History at [redacted] to reserve a seat.

(b) (6)

(b) (3)-P.L. 86-36

6. (U) Community Service

(FOUO) [redacted] and [redacted] will collect Giant "Apples for the Students" tapes this year. [redacted] is collecting for the Ruth Parker Eason school in Anne Arundel Co., and Bob is collecting for the Immaculate Conception school in D.C. If there are other efforts out there you wish to have included in our newsletter, please let us know.

7. (U) PUZZLES

a. (FOUO) Solutions to September puzzles:

Puzzle #0: Tom Swifty (SAID = 6)

A Tom Swifty is a phrase in which what Tom states is punningly related to how he says it; some examples:
"I love sugar in my coffee," Tom said sweetly.
"I'm dying," Tom croaked.

In this problem, you are to replace SAID with a 6-letter word that makes the phrase a nice Tom Swifty.

"Irish wood is the best," Tom SAID.

(b) (3)-P.L. 86-36

[redacted]

I received several answers, but the best is OPINED. This is a pun on both "Irish" (O') and "wood" (pine). Also note that Tom is, in fact, stating an opinion.

(b)(3)-P.L. 86-36

Solutions were received by [redacted]

Puzzle #2: Digital Devil

For each positive integer n, let A_n be the number of digits in the binary representation of n, and let B_n be the number of ones in the binary representation of n.

What is (1/2)^(A_1+B_1) + (1/2)^(A_2+B_2) + (1/2)^(A_3+B_3) + ... ?

Solution:

Note that A_{2n} + B_{2n} = A_n + B_n +1 and A_{2n+1} + B_{2n+1} = A_n + B_n + 2 and so letting
S = (1/2)^(A_1+B_1) + (1/2)^(A_2+B_2) + ...
we see that
S = 1/2^2 + (1/2)^(A_2+B_2) + ...
= 1/2^2 + (1/2 + 1/2^2)*((1/2)^(A_1+B_1) + ...
and so
S = 1/2^2 + S*(1/2 + 1/2^2). Solving for S, we obtain that S = 1.

(b)(3)-P.L. 86-36

Solutions were received by [redacted]

b. (U) November puzzles

Send answers to any or all puzzles to [redacted].

Puzzle #0: Cryptic (7)

Treat this as a clue in a cryptic crossword puzzle, and give the answer:

Aquatic creature cycles briefly to rise.

Puzzle #1: Knuth Knows (rerun from last month due to missing question!)

Donald Knuth, one of the most famous computer scientists in the world (and who was the first published as a kid in Mad Magazine) believes that it is possible to make any positive integer by starting with a single 3 and then using some combination of the operations factorial !, square-root sqrt(), and greatest integer []. Note that n! = 1*2*...*n (e.g. 6! = 720), and that [x] is the greatest integer less than or equal to x (e.g. [3.14] = 3). As an example, we can make 26 by [sqrt((3!)!)], since 3! = 6, 6! = 720, sqrt(720) = 26.8, and [26.8] = 26.

(b)(3)-P.L. 86-36

[redacted]

Show that it's possible to make 10.
For extra credit, make 4 (this is *a lot* harder than it sounds!).

****

Puzzle #2: Making the Grade

Spike is taking a series of exams, and it turns out that he'll have to score a 97 on the last one in order to average 90 for the entire series. But even if he scores as low as a 73, he'll still average an 87. How many exams were in the series? For extra credit, generalize this, i.e., if a difference of x points on the final exam corresponds to a difference of y points in the overall average, how many exams were there in total?

//
##

8. (U) EDITORIAL CORNER

REMINDER: Submissions for the December issue are due by November 22nd.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

(b)(3)-P.L. 86-36

\\\

THE CLASSIFICATION OF THIS NEWSLETTER IS ~~TOP SECRET UMBRA~~

SIGNATURE _____(Required to Verify Ballot)

After completing your KRYPTOS ballot, please fold the lower half of page to the above line, and staple so that the signature is visible.

[redacted]

Return completed ballot to [redacted] HQs, or bring it to the Annual Meeting on Tuesday, November 19th, 1996, at 1300 in Friedman Auditorium.

CANDIDATES FOR PRESIDENT-ELECT
(Vote for one)

_____
_____
_____ (Write-In) _____

CANDIDATES FOR SECRETARY
(Vote for one)

_____
_____
_____ (Write-In) _____

CANDIDATES FOR MEMBER-AT-LARGE
(Vote for two)

_____
_____
_____
_____
_____ (Write-In) _____

[redacted] (b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

[redacted] (b)(3)-P.L. 86-36

[redacted]

(U) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:19
(U) PE EXTERNAL PAGE

(b) (3)-P.L. 86-36

THE CLASSIFICATION OF THIS NEWSLETTER IS ~~TOP SECRET UMBRA~~

****
* TALES OF THE KRYPT *
****
December 1996

//
****

++
//

~~(FOUO)~~ TABLE OF CONTENTS:

1. (U) CA Perspective

2. (U) Calendar of Events

3. (U) CACP News

4. (U) KRYPTOS News

5. (U) Technical Health

6. (U) Community Service

7. (U) Historical Tidbits

8. (U) Puzzles

9. (U) Editorial Corner

//

1. ~~(S)~~ PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature [redacted] D/Chief of Z3.

~~(FOUO)~~ As the R Technology Forecast 96 points out, there is plenty of attention being paid to the "rapidly advancing and continuously evolving telecommunications and computing environment" in which we are working. The CA community understands this firsthand and, as [redacted] said when he recently briefed the Z workforce, "We are an information age organization."

(b) (3)-P.L. 86-36

~~(FOUO)~~ Technology gets the headlines but what about management and the management of change? How well are we doing in these areas? How well are we learning how to manage change and how well are we doing in changing the way we manage? Our successes in these areas are just as important as our successes in keeping up with technology.

~~(FOUO)~~ Managing in the 90's requires a whole new set of skills and an outlook that many of us were neither trained nor prepared for. "Plan, organize, command, coordinate and control" were fundamental to managing in the 70's and 80's. The hierarchy was well-defined and easily understood. Without a hierarchy, how were ambitious people going to measure the climb? That's all changed now. As Scott Adams wrote in "The Dilbert Principle", "I get all nostalgic when I think about it. Back then, we all had hopes of being promoted beyond our levels of competence. Every worker had a shot at someday personally navigating the company into the tar pits while reaping large bonuses and stock options. It was a time when inflation meant everybody got an annual raise; a time when we freely admitted that the customers didn't matter. It was time of joy." Scott certainly has some lighthearted views, but what are some of the serious characteristics of being a good manager in these torrid times?

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

(FOUO) I've got a collection of notes that were taken from reading a pretty broad assortment of contemporary management/leadership books. Some of the titles are really unique: "Leadership When th"e Heat's On", "Teaching th"e Elephant to Dance", "Lincoln on Leadership", Even Eagles Need a Push" and All You Can Do Is All You Can Do". There are some pretty strong and recurring themes spelled out in these books.

(FOUO) The new manager must ask "What for?" Everything must be in question. Everyone must change. Every organization has to prepare for the abandonment of everything it does. If something has been done the same way for three years, there's an 80% chance there's a better way of doing it. When Jim Devine appeared on "Talk NSA" in July 1995, he said "We've had an enormous amount of change in the Agency over the past three years. But for those of you who are hoping that the change will soon come to an end, that things will go back the way they were, that we'll get back in business as usual, that's not going to happen." Change! Down with the past! Revolutionize! Think radically. Lead experimentally. Go out on a limb. Go over the cliff. Sometimes when you're trying to change, however, you break something that's already fixed. That's okay, for unless you change and take the risk of failure, you limit your opportunities for success. That's why questioning, probing, reinventing and changing are so important.

(FOUO) Those of us who grew up in a structured environment have a difficult time accepting ambiguity and uncertainty. Nevertheless, ambiguity and uncertainty are running rampant and we're all faced with the dilemma of trying to understand priorities and responsibilities. Pinning down your job during periods of change can be like trying to nail Jell-O to a wall. We need to take personal responsibility for figuring out the top priorities and pointing ourselves in that direction. Roles may be vaguely defined and assignments altered constantly as priorities shift. People with a high need for structure hate this! Prepare to feel your way along and wing it.

(FOUO) The successful manager today isn't the one who is entrusted with secrets but is the one who wins trust by sharing what he or she knows. It's only when people trust that they can be mobilized. But to gain trust, we must be candid, forthright and open with everybody. To gain that trust you've got to make yourself vulnerable; you've got to give up control. The nice paradox of control is that giving it up is the best way to get it. Leaders know that the more they control others, the less likely it is that people will excel. The real trick, then, is not to command, not to manipulate, but to share information and educate. The reason managers in the private sector can actually manage in today's markets, running the race that begins at top speed and then picks up pace, is that they are not alone. They are "we." "We" with their subordinates (if that is the right word), "we" with their bosses (if that is the right word) and "we" with their peers (which is surely the right word). In some organizations today, the right word is associates, which may be the best word of all.

(FOUO) Managers must have very strong networking skills. Managers must have a big-picture perspective to see how the pieces fit together. They must be good coaches with a real sensitivity to people. They must be open to criticism. They must be thoughtful and deliberate. They must understand that "getting the steel out" is their crew's responsibility. Their responsibility is to take care of that crew. Managers must learn to accept the fact that they have to evolve >from controller to coach, from supervisor to supporter and from administrator to enabler. The manager's primary contribution is in the recognition of good ideas, the support of those good ideas and the willingness to challenge the system in order to get new products, processes and good ideas implemented. Put another way, the role as manager is about three things. Number one is to give employees the tools they need to do their job. Number two is to remove obstacles that hinder team performance. Number three is to challenge the imagination.

(FOUO) If you're a manager today, you've got some pretty heavy responsibilities. If you're being managed, and that means all of us, we've got some pretty high standards that we want our managers to achieve. I've saved three quotes that deal with this:

1. "People cannot be managed. Inventories can be managed but people must be led." H. Ross Perot (I think he said that long before he got into politics....)

2. "Things refuse to be mismanaged long." Ralph Waldo Emerson

(b)(3)-P.L. 86-36

3. "An organization will never rise above the quality of its leadership." Danny Cox (from "Leadership When the Heat's On"). The last quote is what gets me going each day and, I think, is as important as the pace of change in technology.

.....
//

2. (U) CALENDAR

10 Dec	NSA Anti-Terrorist Force Protection Symposium, (Friedman, 1000-1200) (See 6b)
12 Dec	James Boone, former NSA DDR, "An Outsider's View of Your Challenges" (R&E Symposium Center, 1000-1100)

PLAN AHEAD

29 Jan	Breakfast for Newly Certified Cryptanalysts, (BANCC), Canine Suite, time to be announced.
5-9 May	ACE '97 at CCR-Princeton

.....
//

3. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

a. (U) New Professionalization Announced

~~(FOUO)~~ The CACP is pleased to announce that [redacted] got certified this month.

.....

b. (U) CACP Gains New Program Participants

~~(FOUO)~~ Following is a list of those who have joined the CACP family -

Interns:

[redacted]

(b)(3)-P.L. 86-36

Cross-Trainees:

[redacted]

A hearty welcome to all!

.....

c. (U) Third Annual BANCC Plans Underway

~~(FOUO)~~ The CACP and the KRYPTOS Council are pleased to announce preliminary plans for the next BANCC. [redacted] is chairing the event which recognizes those who have been professionalized within the past year. Menu and times will be announced soon.

.....
//

4. (U) KRYPTOS NEWS

a. (U) Election Results Announced

~~(FOUO)~~ At the November meeting the results of the election for new Council members were announced. [redacted] is the new President-Elect, [redacted] is the new Secretary, and [redacted] and [redacted] are the new At-Large Members. [redacted] the out-going President also expressed her thanks to the other Council members whose terms of office had expired, [redacted] Secretary, and [redacted] and [redacted] members-at-large.

(b)(3)-P.L. 86-36

[redacted]

5. TECHNICAL HEALTH

a. (U) CALL FOR ABSTRACTS - ACE 97

(TSCUO) The Annual Cryptomathematics Exchange, ACE, will be held the week of May 5-9, 1997, at CCR in Princeton, New Jersey. ACE is the premier conference for classified cryptomathematics.

(U) The conference will feature both general sessions (talks of general interest) and specialized sessions held in parallel. Conference proceedings will be published containing extended abstracts of the general talks.

(TSCUO) General talks will be 20 minutes in length. They may be classified up to TSC, but may not contain compartmented or source-related material. The audience will come from the US, Australia, Canada, New Zealand, and the UK; including attendees from CCR-LJ, CCR-P, and CCS. All attendees will be eligible to attend all of the general sessions.

(TSCUO) Parallel sessions will provide a forum for continued discussions of the morning's sessions' topics. Discussions in the parallel sessions may be classified up to TSC. All attendees will be eligible to attend all scheduled parallel sessions.

(TSCUO) Those wishing to present a talk at ACE 97 should submit a short abstract to an ACE representative (see below) which must reach [redacted]

by 5 p.m. on FRIDAY, JANUARY 17, 1997.

Australian, Canadian, New Zealand and UK submissions should be made through the appropriate liaison office. The short abstract is 1 or 2 pages in ASCII, and it must be properly classified (including paragraph classifications). The short abstract should also include the title and speaker, the author(s), and the classification of the talk. Furthermore, US personnel must send a signed Conference Approval Sheet (available from the ACE reps) to [redacted]

(TSCUO) Questions should be referred to your ACE representative:

[redacted]

(b)(3)-P.L. 86-36

6. COMMUNITY SERVICE

a. (TSCUO) Personal Cryptology Collection Available to Borrowers
(submitted by [redacted] Z Technical Librarian)

(TSCUO) [redacted] currently assigned to G21/TARS, has lent a number of recent books on cryptology to the Z Technical Library. They represent the kind of techniques that are being disseminated in the public domain today. These are Joe's personal copies but he is willing to let others borrow them. Please see [redacted] Z Technical Librarian, before you remove the books from the shelf.

[redacted]

1. "Cryptography, Theory and Practice", CRC, 1995 by Douglas R. Stinson.

2. "Codes and Cryptography", Oxford, 1988 by Dominic Welsh.

3. "Number Theory and Cryptography", Cambridge, 1990 by J. H. Loxton.

4. "Applied Cryptography", John Wiley, 1994 by Bruce Schneier.

5. "Cryptography and Secure Communications", McGraw, 1994 by Man Young Rhee.

6. "Elliptic Curve Public Key Cryptosystems", Kluwer, 1993 by Alfred Menezes.

7. "E-mail Security: How to Keep Your Electronic Message Private", John Wiley, 1995 by Bruce Schneier.

8. "Computer Communications Security", Prentice Hall, 1994 by Warwick Ford.

9. "PGP: Pretty Good Privacy", O'Reilly, 1995 by Simson Garfinkel.

10. "Protect Your Privacy: A Guide for PGP Users", Prentice Hall, 1995 by William Stallings.

11. "Security Architecture for Open Distributed Systems", John Wiley, 1993 by Sead Muftic, Ahmed Patel, Peter Sanders, Rafael Colon, Jan Heijnsdijk and Unto Pulkkinen.

12. "PGP: Pretty Good Privacy" (in German), 1994, by Philip Zimmermann.

13. "ZCONNECT: Das Datenaustauschformat fur mailbox-netze", (German) 1965 by Wolfgang Mexner, Felix Heine, Matthias Jung, Hartmut Schroder, Martin Husemann and Rena Tangens (this shows how PGP is integrated into Z-NETZ).

14. "Zerberus: Das mailbox-UserInnen-Handbuch", (German), 1992 by Matthias Jung.

15. "Contemporary Cryptology: The Science of Information Integrity", IEEE, 1992 by Gustavus J. Simmons.

.....

b. ~~(S-CCO)~~ NSA Anti-Terrorist Force Protection Symposium

~~(S-CCO)~~ To all fully cleared (TS/SI) personnel: Please join us for a DIRNSA-sponsored half-day symposium focusing on the timely and important issue of Anti-Terrorist Force Protection. The symposium will take place on 10 December, from 0900 - 1200 in the Friedman Auditorium, with remote broadcast to FANX III. While co-sponsored by W9B and ADDO/MS, the symposium will touch on all major lines of business within the NSA and service cryptologic communities.

Proposed Agenda and Distinguished speakers will include:

Opening remarks: Mr. Rich Taylor, NSA EXDIR

Key note address: [redacted] DASD/I&S (b)(6)

Brigadier General [redacted] JCS/J34

[redacted] (b)(3) - 10 USC 424

NSA Anti-Terrorist Force Protection Issues/Initiatives

NSA Anti-Terrorist/Force Protection Expert Panel - Q & A Session

Closing remarks: Brigadier General [redacted] ADDO/MS (b)(1) (b)(3)-P.L. 86-36

[redacted] (b)(3)-P.L. 86-36

[redacted]

[redacted] (b)(1) (b)(3)-P.L. 86-36

(U) For more information call [redacted] or [redacted]

c. Apples for the Students

(FOUO) [redacted] and [redacted] (b)(3)-P.L. 86-36 will collect Giant "Apples for the Students" tapes this year. [redacted] is collecting for the Ruth Parker Eason school in Anne Arundel Co., and Bob is collecting for the Immaculate Conception school in D.C.

7. (U) HISTORICAL TIDBITS

a. (U) The Strip Cipher Device (CRYPTOLOGIC ALMANAC)
(David A. Hatch, Director, Center for Cryptologic History).

(U) On 6 November, NSA hosted a visit by [redacted] who has been heavily involved in restoring Bletchley Park -- wartime home of British cryptology -- and rebuilding COLOSSUS, one of the world's first computers. [redacted] made two informative presentations on Anglo-American cryptologic operations during World War II. On the occasion of this visit, Mr. William Crowell, NSA's deputy director, presented [redacted] with an M-138-A strip cipher device for display at Bletchley Park. (b)(6)

(U) Here is a little background on the strip cipher device.

(U) The idea for a strip cipher device goes back to 1915. Captain (later Colonel) Parker Hitt of the Army Signal Corps conceived the idea for a "flat" version of a cylindrical cipher device he had invented. When the idea was not adopted for official work, Hitt and his wife used the "flat" device for their personal correspondence for many years.

(U) The idea for a "flat" device surfaced again in the 1930s, as the U.S. Army and Navy began searching for a cipher system for low echelon communications during joint operations. When the Army proposed its cylindrical device, the Navy objected: the alphabets were permanently engraved on the cylinder and could not be changed. After some discussions, William F. Friedman, the Army's senior cryptographer, proposed a flat board with interchangeable sliding strips of paper on which the cipher alphabets were printed. The Navy agreed in principle.

(U) Friedman and his associates began working out doctrine for use of the device. Solomon Kullback, who had special expertise in statistics, worked out the "maximum use limit" for a strip cipher of 25 randomly mixed alphabets. Friedman's associates tested the device against a variety of mathematical attacks and found it secure. The final design had two aluminum plates, hinged like a book, holding 25 paper strips on which were printed alphabetic mixes.

(U) Frank Rowlett, another of Friedman's associates, was proud of the cryptographic strength built into the device. To the chagrin of the Army cryptographers, however, when the strip cipher device was used in a training class to give cryptanalytic trainees a realistic and frustrating exercise, a pair of officers solved messages easily and recovered all the alphabets used in the underlying device. The officers had made clever -- and correct -- assumptions about repetitions at the beginning of the test messages. This experience led to revisions in how the device was used.

(U) The Army adopted the device in July 1934, the Navy in January 1935. Both used it until 1947.

(U) Strip cipher devices were somewhat slow in operation, but they had several advantages. Primarily, they were relatively inexpensive and relatively easy to distribute. Moreover, if one device were compromised, it was less serious to the system as a whole than the loss of a sophisticated machine would be. Therefore, in 1942 the U.S. Army ordered 5,000 strip cipher devices. The Navy also ordered them in great quantity. (b)(3)-P.L. 86-36

[redacted]

(U) The strip cipher device was also issued to many nonmilitary government organizations. The State Department, Treasury Department, and the OSS used it, among several others. During the war, the device was also issued to several Allied governments to facilitate interallied communication; Great Britain and the Soviet Union were among the recipients.

(U) This device was strong but not invulnerable. Therefore, it was used to protect only low echelon communications and as a backup for the stronger machine systems in the U.S. inventory. Nonetheless, it was an important component of the cryptographic security that saved many thousands of American and Allied lives during World War II.

****

b. (U) New Archival Assessions Announced

1. WILLIAM FREDERICK FRIEDMAN (Accession #47270)

(TSC) William Frederick Friedman was a cryptanalyst, scholar, author, teacher, cryptologic pioneer and inventor. "Mr. Friedman (1891 - 1969,) was the dean of modern american cryptologists, the most eminent pioneer in the application of scientific principles to cryptology who laid the foundation for present-day concepts. He was born in Kishinev, Russia, on September 24, 1891, he came to the United States in 1892; he retired from NSA in 1955 after 35 years with U.S. cryptologic activities, and died at his home in Washington D.C., on November 2, 1969" - Lambros D. Callimahos. This accession in the NSA/CSS Archives consists of material from Mr. Friedman's personal files, some having been retrieved from his residence. The record includes speeches, presentations, publications, newspaper articles, patent information, personal information, correspondence, photographs, diaries, letters, etc.

2. LAMBROS D. CALLIMAHOS (Accession #47271)

(TSC) Lambros D. Callimahos was a senior cryptologist. He was born in Egypt on December 16, 1910, and he came to the U.S. when he was four years old. At the time of his death on October 28, 1977, he was reputed to be a world renowned flutist, distinguished cryptanalyst, instructor, linguist and author. During his time at NSA, he served as a technical consultant to William Friedman and an instructor of CA-400, "Intensive Study in Cryptanalysis." He left NSA with 27 years of service. This accession in the NSA/CSS Archives consists of papers, photographs, slides and microfilm.

//////////

8. (U) PUZZLES AND PROBLEMS

a. ANSWER TO MARCH 1996 POM (A number of people requested this)

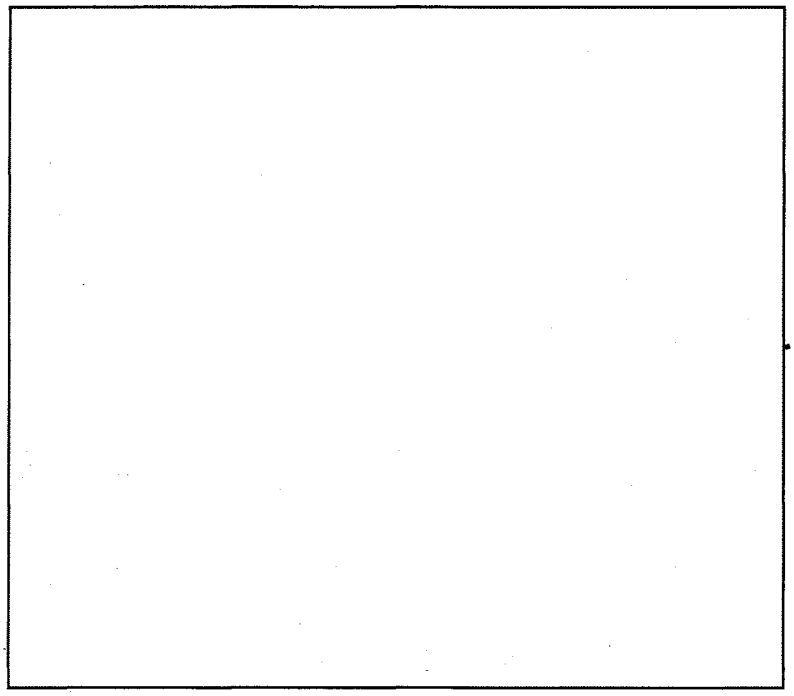
(TSC) It has been a long time since this problem was published so I am repeating the cipher. To my knowledge, [redacted] was the only person to solve this cipher.

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

b. (U) December Puzzle

1. Solutions to November puzzles:

Puzzle #0: Cryptic (7)

Treat this as a clue in a cryptic crossword puzzle, and give the answer:

Aquatic creature cycles briefly to rise.

Solution:

MANATEE. The clue "aquatic creature" refers to "manatee" and the clue "arise" refers to "emanate". Finally, the clue "cycles briefly" refers to the fact that we cycle the letters in "manatee" by a small amount (in this case, 1 letter).

Solutions were received from [redacted]

Puzzle #1: Knuth Knows (rerun from last month due to missing question!)

Donald Knuth, one of the most famous computer scientists in the world (and who was the first published as a kid in Mad Magazine) believes that it is possible to make any positive integer by starting with a single 3 and then using some combination of the operations factorial !, square-root sqrt(), and greatest integer []. Note that n! = 1*2*...*n (e.g. 6! = 720), and that [x] is the greatest integer less than or equal to x (e.g. [3.14] = 3). As an example, we can make 26 by [sqrt((3!)!)], since 3! = 6, 6! = 720, sqrt(720) = 26.8, and [26.8] = 26.

Show that it's possible to make 10.
For extra credit, make 4 (this is *a lot* harder than it sounds!).

(b)(3)-P.L. 86-36

Solution:
Let S denote square root, ! denote factorial, and [] denote greatest integer. We can get the following:
10 = [S[SS(3!!)]!]
7 = [SSSSSSSSSS(3!!!)]
8 = [SS(7!)]
14 = [SS(8!)]
4 = [SSSS(14!)]

[redacted]

Other solutions are possible.

Solutions were received from [redacted]

Puzzle #2: Making the Grade

Spike is taking a series of exams, and it turns out that he'll have to score a 97 on the last one in order to average 90 for the entire series. But even if he scores as low as a 73, he'll still average an 87. How many exams were in the series? For extra credit, generalize this, i.e., if a difference of x points on the final exam corresponds to a difference of y points in the overall average, how many exams were there in total?

Solution:

Let S be the sum of all of his exam scores before the final, and let there be a total of n exams. Then we have $(S+97)/n = (S+73)/n + 3$, or $3n = 24$, and so, $n = 8$. In general, if a difference of x points on the final exam corresponds to a difference of y points in the overall average, there are x/y exams in total.

Solutions were received from [redacted]

(b)(3)-P.L. 86-36

---

c. (U) KRYPTOS KRISTMAS KWIZ!!!!!!!!!!!!!!!!!!!!!!

(FOUO) This will run for two months (i.e. there won't be a new puzzle in January). Deadline for submission of answers is January 10. "Tales of the Krypt" readers please submit solutions to [redacted], except for those at GCHQ, who have their own instructions. Name of the winner will be printed with score in the February issue of TOTK, along with names of all others who submitted answers and obtained a score greater than zero. Combined entries are certainly allowed, and you may continue to submit solutions up until the January 10 deadline. The hoped for prize is a Bletchley Park mug, if the winner is a single person, or pins if the winning entry is from a team.

(FOUO) [redacted] have again put their warped minds together to produce the 1996 Kryptos Kristmas Kwiz, designed to keep you from all the things you OUGHT to be doing (work, Christmas shopping, etc). As before, some questions are more difficult than others, so each has an associated Warp Factor. For factors greater than 1, points may be awarded for a nearly-correct answer or even a gallant effort, so enter something on the answer sheet even if you're not sure. And if your answer is better than ours, you may receive bonus points. We think that this year's quiz is at least as difficult as last year's, so do return your answer sheets, even if they are incomplete.

(U) Merriam Webster's Dictionary will be taken as the authority for what constitutes a "word". If your answer includes an obscure word which is not in Merriam Webster's but in some other common dictionary, tell me which. Unless otherwise stated, "words" do not include proper nouns or entries which contain punctuation (hyphen or apostrophe).

(U) So, good luck, and have fun!

(b)(3)-P.L. 86-36

1. Where does "heaven" fit in the following list (read across lines in order):

hound	art	blood	bread	strap	lantern	heel
pastry	manger	bucket	wool	wig	grease	column
class	ointment	soldier	dimension	leave	belt	matter
shake	flask	summer	box	cap	cross	moon

[redacted]

hole	wood	bag	peel	neck	sky	gin	
brick	hand	dark	blade	sense	fly	roll	
world	hole	night	century	collar	watch	pages	(5)

2. Compile a list of 16 8-letter words, such that the last four letters of each word (except the last), followed by the first four letters of the next word, also spell a word. (2)

3. A WithWord is a word which can precede a list of other words to produce a further set of words, which may be hyphenated. For example, the WithWord associated with [bid, break, burst, cast, crop, door, fit] is OUT. What are the WithWords for the following sets:

[foot, horse, house, ship, weight, year]

[able, box, day, house, mate, shop, shy]

[boat, bow, division, hand, range, standing]

[army, line, lord, mark, mine, slide]

[blind, chat, crop, dead, wall, ware]

[age, date, drake, drill, made, power]

[age, fish, it, master, saw, stand] (1)

[going, ion, rush, set, side, to, us]

What WithWord is associated with these eight WithWords? (1)

4. The inhabitants of the planet Corrigenda use the same digits as we do, and representing the same quantities, but they use different words for "plus", "minus", "times", "over" and "equals". Curiously, their five words are the same as ours but with different meanings. Determine which is which from the following, and complete the second equation (note that operations are left to right: 6 - 4 / 2 = 1, not 4):

2 equals 6 minus 4 plus 3 times 1

4 over 7 times 3 minus 5 plus ? (1)

Construct an equation containing the five operators at least once each which is valid on both Corrigenda and Earth. (1)

5. In the Good Old Days of telex, plain text was punched onto 5-level paper tape, often using the following codings (in binary order): 7T3O9HNM4LRGIPCVEZDBSYFXAWJ5UQK8 (where the digits represent various teleprinter functionals). Thus T had a hole punched only in the fifth level, I had holes punched in the second and third levels, and 8 had holes punched in all levels. Interpret the following stream:

89RZ78SFL7E4M4E78SS47EE8EE7CZZC74YY377789RZ78SFL7Z8Z74YY37EE8EE7

849487OISIO74YY377789RZ7KTNTK7Z8Z7

What follows? (1)

6. What is the next number in the following series:

(a) 1 2 3 5 10 19 20 30 50 100 190 200 (1)

(b) 3 7 12 14 16 19 21 25 30 41 45 52 54 56 (1)

(c) 8 13 17 22 24 26 29 31 35 42 44 46 49 53 (1)

(d) 1 5 11 15 20 40 51 55 60 90 102 104 106 109 (2)

7. A stepword is a word of 2 or more letters in which one letter can be stepped, incrementally, through the cyclic alphabet, to form other words, eg CONE CORE COVE COZE CODE.

(a) what stepword gives the longest such list? (1)

(b)(3)-P.L. 86-36

(b) what 8-long stepword gives the longest list? (1)

8. Four balls, each with a radius of 1 inch, are arranged in a square, on a flat surface, with each ball touching its neighbours. A fifth ball, of the same size, is placed on top of these four, so that it is supported by each of them. What is the vertical distance from the top of the upper ball to the surface (correct to two decimal places)? (2)

9. If you can dramatise: unwills, foliate, gumshoe, weakest, respect, scaredy

then:

a. illustrate: comical, echelon, spangle, ocelots

b. calculate: impiety, Warrell, inferno, Sumatra (1)

10. A recent (1992) reference book has a section which contains a list of 42 "things". 15 ars UK and 14 are US; Australia, Austria, Germany and Italy have 2 each, and Canada, Israel, Netherlands, Norway and USSR have 1 each. The oldest is Italian (1778), the most recent UK (1973). What are they? (1)

11. Fred Bloggs was pleased with himself. He had devised a method for enciphering messages on his PC, using nothing but a simple algorithm and a "secret" key. He sent a test message to his pal Joe Blow, and the following exchange was observed:

TO: JOE BLOW FM: FRED BLOGGS

XDARD LDASB PCASG VHIHP ZYTGH VFMVD JJZIW MKXCX FXYMT LPDQX

RDBPL PEZAD IUHNO NJLBG RUWBE IURBD QKRBI VSUMX OGTMZ WBORX

NFAFK DHWGW ASTHK RDKOU JHAVV

TO: FRED BLOGGS FM: JOE BLOW

EXAYN ACGGB UHKNL BRTDD RLDYR XAQAY SPTNQ DJKKO KBOKI

TO: JOE BLOW FM: FRED BLOGGS

WDARD LDASB OCASG VHIHO YYTGH VFMUB IJZIW MKWZU EXYMT LOZKT

QDBPL OZPQY HUHNN HURMA QUWAX NLIGW PKQTG RAQKP NFKCT AFIHO

LVHPI LPGNL OPKPQ XLBKX UVZJH

TO: FRED BLOGGS FM: JOE BLOW

EXAYZ KEPSZ IIGRL PWHGD VJUPR IUCHC IDFMG BDOZF

(a) What does the last message say? (2)

(b) What did Fred do wrong in the first message? (3)

12. What is the next value in the following series:

(a) 1 4 8 13 21 30 36 45 54 63 73 85 95 (1)

(b) -2 -1 -2 0 1 3 2 3 5 7 5 6 5 6 8 9 8 10 11 (1)

(c) -2 -3 -1 0 2 1 2 4 6 4 5 4 5 7 8 7 9 10 13 (1)

(d) 4 5 8 8 9 9 12 13 13 13 17 18 21 22 22 23 26 26 27 (1)

(e) 2 5 8 10 13 17 18 20 25 26 29 32 34 37 40 41 45 50 (1)

(f) 1 2 5 13 34 89 233 610 1597 (1)

(g) 7 8 5 5 3 4 4 (1)

(b)(3)-P.L. 86-36

(h) 11 25 34 41 56 63 71 85 92 107 114 (2)

13. The following figures give the approximate answer, and the exact answer (in parentheses), in that order, to what question?

.37 (0) .74 (1) 2.21 (2) 8.83 (9) 44.15 (44) 264.87 (265) (2)

14. A square is inscribed in a circle which is inscribed in a square which is inscribed in a circle which is inscribed in a square. What is the ratio of the areas of the largest and the smallest squares? (1)

15. Which is the odd man out?

(a) ARGON HELIUM KRYPTON NEON NITROGEN RADON (1)

(b) CHEETAH GIRAFFE GNU GORILLA LEOPARD LION TIGER ZEBRA (1)

(c) ALTMAN BOGDANOVICH COPPOLA KUBRICK POLANSKI SCORSESE SPIELBERG (1)

(d) BRASILIA COLOMBO HAVANA KHARTOUM ROME STOCKHOLM TEHRAN OTTAWA (1)

(e) ARTEMIS DEMETER EOS HECATE HERA MORPHEUS PERSEPHONE SELENE (1)

(f) AMIENS ANTWERP FLANDERS JUTLAND LOOS MARNE SOMME VERDUN YPRES (1)

(g) ARMENIA BULGARIA BURMA COLOMBIA ESTONIA ICELAND JAPAN NORWAY (1)

(h) which is the odd man out of the odd men out? (2)

16. A set of items is arranged in an obvious order and numbered 1, 2 etc., and the following observations are made:

(a) 1 and 4 also appear in a different set, which contains 24 items, also at positions 1 and 4;

(b) 3, 10, 13, 15, 18 and 22 nominally have something in common, but 10 and 22 are most closely associated;

(c) 9, 12 and 17 appear in different parts of the world;

(d) 6 and 20 are two of a kind.

What colour was a 25 21? (1)

17. What can be defined as:

(a) A figure of speech where a deliberate understatement is made for the sake of effect, e.g., "he made a very "decent" contribution". (1)

(b) A figure of speech where there is a deliberate use of exaggeration for the sake of effect, as in the phrase "tons of money". (1)

(c) The separation of the parts of a compound word by a word or words, e.g., Piccabloodydilly Circus. (1)

18. (a) If 2**(m) - 1 and 2**(n) are its factors, who wrote the book? (1)

(b) Who directed the film whose title contains a 4-digit number which has precisely three factors under 30 (excluding 1), all prime? (1)

19. What connects the following?

"The English Palladio"; noted seafarer and colonist who died in 1631; "the Empress of the Blues"; actress in "A farewell to Arms" and "Towering Inferno"; actress in "The Pumpkin Eater" and "A Room with a View"; actor in "Conan the Barbarian" and "The Hunt for Red October"; Astronomer Royal 1933-1955; pop singer, born Pontypridd in 1940; Scottish novelist who wrote "Murdo and Other Stories"; and 200m World Championship winner in 1983/87. (1)

20. By what names are/were the following better known:

(b)(3)-P.L. 86-36

9/23/2010

(a) Doris von Kappelhoff (b) Allen Stewart Konigsberg

(c) Charles Lutwidge Dodgson (d) Frederick Austerlitz

(e) Jean-Baptiste Poquelin (f) Amandine Aurore Lucille Dupin (3)

21. Apart from being names, what do the following have in common:

ALICE CICELY ELAINE ESTHER JANE JASON MARIAN NORMA RONALD (1)

22. What is the longest pair of words you can find which give another word when the letters are added, mod 26, in order. Take your choice - A = 0 or A = 1 (so that A + A can give A, or B) - but be consistent! Example: CAT + BED = DEW. (1)

23. Language is highly redundant - for example one can omit all the vowels from a text and it is still (mostly) readable: eg K-NG S-L-M-N'S M-N-S. Work out the following book titles.

(a) -O-I-S-N -R-S-E alternate letters

(b) - --R-W--- TO -R-S second half of the alphabet only

(c) ---- A-D L--E-- first half of the alphabet only

(d) --- --- I- --- -I-- -- I--- ---I---I-- only the letter I (2)

24. [Unfortunately the instructions for this question got lost, but see if you can solve it anyway. We believe the text is complete].

"We enjoyed a Buck's Fizz before the meal. We found the roast quail a most satisfying starter; then it was a pure pleasure to eat lamb "a l'Italiano", gnocchi and seasonal vegetables. Then the sweets: dairy selection - yoghurts or fromage frais (surely the perfect item to cleanse the palette) - or banana mousse, eclair eglantine (the chef's creation, and a clear sign of his inventiveness and experience). Then coffee, regular or expresso; a large selection of savoury fare - gingerbread pieces, each extraordinarily shaped like a man, a plate of petit-fours, and nuts. A perfect end to the day: bill paid (nice tip included), and now it's time to go to bed."

How many? (please list them) (1)

25. The following are solutions to the equation a**2 + b**3 = c**2 + d**3, where a, b, c and d are 4 positive integers and a is not equal to c (for compactness, A=1...Z=26): DACB HAAD IBED JBIC KBBE LAID JECF OBMD OCFF QBIF QCJF SCRD UBRE TDKG UDQF WBEH VDFH XASF WDIH YBKH WFDI ZEQH SHLI and of course CBDA....LISH. Replacing the values of a, b, c and d by literal equivalents in a hatted alphabet of your choice, write down the longest list of 4-letter words you can construct. (3)

26. On what basis are the following countries divided into sets:

(a) (i) India Jamaica Mexico Philippines Venezuela

(ii) Angola Australia Bolivia Fiji Tanzania (1)

(b) (i) Chad France Spain

(ii) Denmark Iceland Thailand

(iii) India Italy Syria

(iv) Algeria Eritrea Tunisia (1)

(c) (i) Australia Japan

(ii) Canada Denmark

(iii) Sweden USA

(iv) Mexico Norway

(v) Italy Mauritania

(b)(3)-P.L. 86-36

(vi) Argentina Syria (1)

(d) (i) Fiji Peru Italy

(ii) Egypt Japan Morocco

(iii) Angola Cuba Poland

(iv) Algeria Kenya Thailand

(v) Belgium Brazil Finland

(vi) Iceland Romania Sweden

(vii) Denmark Ethiopia Uruguay (1)

(e) (i) Afghanistan Algeria Argentina Australia Burma Canada Iraq Romania

(ii) Brazil Egypt France Indonesia Iran Mexico Nigeria Thailand (1)

(f) (i) Denmark Germany Greece

(ii) Belgium Finland Poland

(iii) Angola Austria Turkey

(iv) Canada Hungary Portugal

(v) Brazil Norway Sudan

(vi) Panama Peru (2)

27. And still on the subject of countries, what is the longest list of countries you can compile such that the last two letters of one are the same as the first two letters of the next, in order? (1)

28. What is the longest (not blatantly contrived) sentence you can write containing only four different letters of the alphabet? Common proper names are allowed. (2)

29. Answer the following clues lexicographically:

(a) Notice the best chooses a job (4) (1)

(b) Bomb maddened infuriated nobleman (7) (1)

(c) Discover partisan coordinate system (9) (1)

(d) Making aware of changing fundamental connecting shape (8) (1)

(e) Figure of speech poet found in smallest rooms (7) (1)

(f) Madness, thought at fault, moved slowly (6) (1)

30. Find three different monosyllabic 4-letter words which become trisyllabic 5-letter words when a letter is added:

(a) at the beginning (1)

(b) at the end (1)

(c) somewhere in the middle (2)

31. Find a monosyllabic 3-letter word which becomes a trisyllabic 4-letter word when a letter is added at the end. (1)

32. My first is in Finland but not in Finnish

(b)(3)-P.L. 86-36

9/23/2010

My second is in Holland but not in Dutch

My third is in Albania but not in Albanian

My fourth is in Sweden but not in Swedish

My fifth is in Germany but not in German

My sixth is in Iceland but not in Icelandic

My last is in Wales but not in Welsh

My whole is in England but not in English

Where am I? (2)

33. There is a well-known puzzle in which you are required to construct as many integers as possible using just four 4s and the operators + - * /, together with brackets, decimal points, factorials, roots, indices and recurring decimals. Thus:

```
12 = ((4! - 4) * .4) + 4
32 = sqrt(.4) * (44 + 4)
and 63 = (4**4 - 4) / 4
```

In this version you have all the same rules, but the only digits used must be 3, 3, 5 and 5. So for example 10 = (35 - 5)/3 or 35/3.5

Construct all the numbers from 180 to 189 inclusive. It is acceptable not to use all four digits, should it be possible. (6*)

* half a point for the first eight, a point each for the last 2

34. An encryption system works as follows: take a piece of text which includes all the letters which you wish to encipher, and number each letter in turn, 1 for the first letter, 2 for the second, and so on. Then replace each letter in the message by the number which is associated with that letter. Where the letter appears more than once in the text, use each of the numbers in turn, cyclically.

Choosing a well-known phrase for the text, a message enciphers to:

13 11 12 6 21 1 2 3 26 6 19 24 14 15 10 30 29 29 35 22 34 33 19 28 13

1 11 7 15 19 3 26 22 1 27 24 30 6 33 34 14 26 2 28 20 30 25 1 32

What is the last word of the message? (2)

35. The following clue leads to 7 4-letter words - but what is the real (two-word) message?

Weaponry thought to damage, left on boat, dictates that I conquered German river. (2)

****

##########

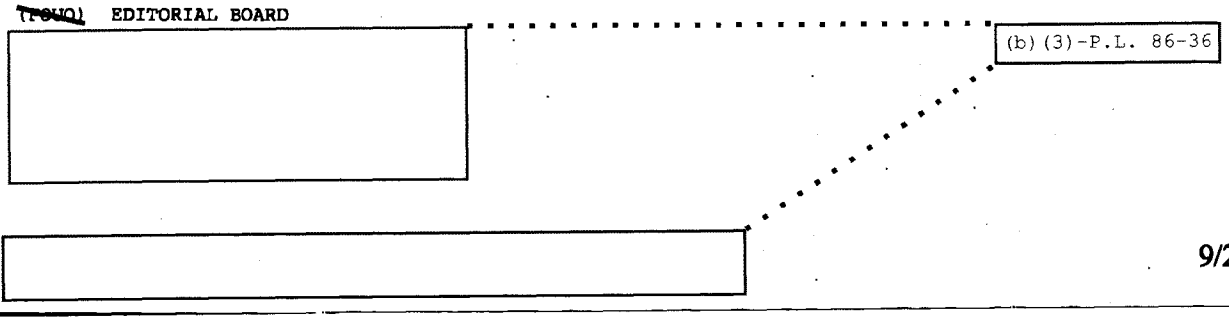
9. (U) EDITORIAL CORNER

REMINDER: Submissions for the January issue are due by December 30th.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

(FOUO) EDITORIAL BOARD



[redacted]

Jack Ingram, Cryptologic History Museum, [redacted] (b)(3)-P.L. 86-36

[redacted]

\\\

TOP SECRET//COMINT

(C) [redacted] *info*
(U) *Last Modified: 10/30/2002 11:42:21*
(U)PE EXTERNAL PAGE

THE CLASSIFICATION OF THIS NEWSLETTER IS ~~TOP SECRET UMBRA~~

(b)(3)-P.L. 86-36

```
**********************************
*        TALES OF THE KRYPT      *
**********************************
```

January 1997

//
****

++
//

(~~FOUO~~) TABLE OF CONTENTS:

1. (U) CA Perspective

2. (U) Calendar of Events

3. (U) CACP News

4. (U) Community Service

5. (U) Editorial Corner

//

1. (~~C~~) PERSPECTIVES IN CA - Each month this newsletter features the perspective of a CA Senior on a CA topic of his/her choice. This month we are pleased to feature [redacted], the Director of IDA-CCR-La Jolla.

~~~~~~

"PERSPECTIVES IN CA FROM CA"

(~~FOUO~~) My first, and perhaps most important, message for you is that CA is alive and well, indeed thriving, in Southern California. To amplify on this I am tempted, given the time of year I am writing, to mimic Dickens with a "KRYPTOS KAROL" giving views of the past, present and future.

(b)(3)-P.L. 86-36

PAST:

(~~C-CCO~~) Cryptanalysis began in California in 1952 when the first "SCAMP" summer program was held at UCLA. This was the very same year that NSA was founded, replacing the AFSA (Armed Forces Security Agency). For the next few years SCAMP moved around from site to site, until in 1959 IDA-CRD was created in Princeton, in part as a permanent home for future summer programs. Later on, in 1968, 1979 and 1983,

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704
~~~~~~

summer programs were held in Monterey, CA, at the Naval Postgraduate School. [redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(C-CCO)~~ During this summer of 1988, support for an earlier-floated idea for a California branch of IDA gained momentum, mainly through the enthusiastic backing of DIRNSA Studeman. One of the main motivations for this was to "foster strong technical interactions with the West Coast academic community." After a feasibility study, the Center for Communications Research-La Jolla (CCR-LJ) was founded in 1989 (with [redacted] as first director), and CRD was renamed CCR-P at the same time, (in fact at the time of its 30th anniversary). Groundbreaking for our permanent facility was held in 1991 and the facility was completed in 1992, about the time I took early retirement from UCLA and moved down here as director. The first SCAMP in our new building was held in the summer of 1993.

(b) (3)-P.L. 86-36

~~(C-CCO)~~ We were fortunate to attract to our initial permanent staff [redacted] We are confident that our newer researchers will do work of equivalent stature.

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

PRESENT:

[redacted]

~~(C-CCO)~~ We currently have a research staff of [redacted] In addition we have about [redacted] regular consultants (technically, "adjunct staff members") from local universities. We also have a support staff of about [redacted] During the summer our SCAMP program brings in about [redacted] visitors from universities for a 10-week period along with [redacted] Hence summers are quite crowded - but exciting!

~~(FOUO)~~ Management is minimal - a director (me), a deputy director [redacted], and a head of admin/security [redacted] Scientifically we report to [redacted] at NSA (head of R51, math research) and, through him, to other NSA offices. Administratively we report to IDA headquarters in Alexandria - IDA is a "federally funded research and development center" running the CCR's (and CCS) under an

(b) (3)-P.L. 86-36

[redacted]

NSA contract.

FUTURE:

(~~S-CCO~~) [redacted] The challenge for the future is to continue to recruit the very best analytic minds into our work; to maintain and increase contacts with the US academic community, especially in the western part of the country; to expand the scope of our research activity to cope with rapidly changing communications environments; [redacted]

[redacted]

[redacted]

[redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

2. (U) CALENDAR

(b)(3) - 10 USC 424

Jan 9 S&E Society Presentation, [redacted] of the National Reconnaissance Office, "The Next Generation Architecture for Space", (1000, R&E Symposium Center) (see 4b)

Jan 29 Breakfast for Newly Certified Cryptanalysts, (BANCC), Canine Suite (see 3b)

PLAN AHEAD

May 5-9 ACE '97 at CCR-Princeton

Oct 29-31 Seventh Symposium on Cryptologic History (see 4a)

(b)(3)-P.L. 86-36

[redacted]

3. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

a. (U) CACP Announcements

1) (~~FOUO~~) Congratulations to the following people who achieved professionalization in CA during December:

[redacted]

~~~~~~

2) LOGO CONTEST

(U) A logo has been chosen for the Cryptanalysis Career Panel. It depicts a cipher wheel with the NSA seal on the end, and the setting CACP, with alphabets based on the keyword CRYPTANALYSIS. Look for this logo in the future on our home page and award plaques. Thanks to all who participated in the contest!

~~~~~~

3) CQB SCORES SOUGHT

(~~FOUO~~) If you are willing to participate in a study of how well CQB scores predicted success in cryptanalysis, and have a copy of your scores for the CQB 1 test, please contact [redacted] or at [redacted]. The results of this study will contain no names, so anonymity will be guaranteed.

(b) (3)-P.L. 86-36

"""

b. (~~FOUO~~) Third Annual BANCC Plans Underway

WHEN: Wednesday, January 29, 1997
8:00 to 10:00 a.m.
Breakfast Buffet is scheduled to be ready by 8:00!

WHERE: Canine Suite

COST: $6.00

Breakfast Buffet Menu:
Traditional Scrambled Eggs
Crisp Bacon
Sausage Links
French Toast
Homemade Biscuits
Hash Brown Potatoes or Cinnamon Apples
Juice
Selection of Teas
Freshly Brewed Coffee

List of Honorees:

[redacted]

[redacted]

[redacted] (b)(3)-P.L. 86-36

Sign up and pay $6.00 to one of the following people by Friday, January 24, 1997:

[redacted]

4. (U) COMMUNITY SERVICE

a. (U) Seventh Symposium on Cryptologic History

(U) The National Security Agency will sponsor and host the seventh Symposium on Cryptologic History, 29 to 31 October 1997 at NSA. The conference will focus on cryptologic history based on recently declassified materials from World War II and the VENONA releases.

(U) The Center for Cryptologic History welcomes papers and panels relating to any aspect of cryptologic history based on research into declassified materials.

(U) To propose either a complete session or individual paper you should submit:

a) a one-page abstract for each paper
b) a one-page statement of session purpose for a panel; and
c) a brief vita for each presenter to:

Dr. David A. Hatch, Chief
Center for Cryptologic History (S542)
National Security Agency
9800 Savage Road, STE6886
Fort George G. Meade, MD 20755-6886

(b)(3)-P.L. 86-36

Telephone: [redacted] Fax: [redacted]

b. (U) Science and Engineering Society Presentation

(U) On Thursday, 9 January 1997, at 10:00 A.M. in the R&E Symposium Center, the Society will present [redacted] of the National Reconnaissance Office speaking on

(b)(3) - 10 USC 424
OGA

NRO

"The Next Generation Architecture for Space"

(U) This presentation will examine the forces requiring new spacecraft design and some of the emerging technologies that will enable the design of small, lightweight, extremely capable systems. [redacted] is currently serving as the Associate Director of the Advanced Technology

[redacted]

Group at the National Reconnaissance Office. He has spent approximately 20 years in the Air Force community. He holds Bachelor of Science degrees in Meteorology and Physics and a Masters degree in Physics.

(U) This presentation will be broadcast on Newsmagazine Channel 17.

~~(FOUO)~~ For information on or membership in the Science and Engineering Society contact Tom Kline [redacted]

BLUE/(OLD GREEN) BADGED PERSONNEL ONLY (b)(3)-P.L. 86-36

***

~~TOP SECRET//UMBRA~~

(~~S~~) *POC:* [redacted] *info*
(U) *Last Modified: 10/30/2002 11:42:21*
(U)PE EXTERNAL PAGE

(b)(3)-P.L. 86-36

THE CLASSIFICATION OF THIS NEWSLETTER IS ~~TOP SECRET UMBRA~~

****
* TALES OF THE KRYPT *
****
February 1997

//
****

++
//

(~~FOUO~~) TABLE OF CONTENTS:

1. Perspective

2. Calendar of Events

3. KRYPTOS News

4. Word from the CACP

5. Technical Article

6. Community Service

7. Problems and Puzzles

//

1. (~~S~~) PERSPECTIVES - Each month this newsletter features the perspective of a Senior on a topic of his/her choice. This month we are pleased to feature [redacted] ment.

~~~~~~

"NSA and the World's Largest Machine" (b)(3)-P.L. 86-36

(~~FOUO~~) The world telecommunications infrastructure has been described as the "world's largest machine". It owes its existence to our insatiable need for information and communication. At the most basic level this machine has become essential to our way of life. It is also an instrument for those who wish to endanger our nation and the lives of its citizens. Information superiority means putting this machine to work for the US and its allies. NSA's success in using the world's largest machine to enhance the security of our nation and its allies depends almost entirely on how rapidly we can change. Collective change, being the sum total of the magnitude and direction of each individual's change contribution, means that we all have a part to play.

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704
~~~~~~

(FOUO) Our need to change is dictated by gross changes in world demographics, economics, politics and technology. In 1994 world international circuit capacity totaled approximately 25 Gb/s. Today the capacity is about 100 Gb/s and by the year 2000 the capacity is expected to reach 250 Gb/s. In 1983 the cost of satellite communications was half that of submarine cable. Today it is five times more expensive and by the year 2000 it is forecast to be 25 times more expensive than high capacity fiber optic cable (based on the cost of transatlantic links). In 1994 there were about 70 million more users of FAX than e-mail. By the year 2000 the number of e-mail users will exceed the number of FAX users by over 70 million. The number of leased lines being installed worldwide is decreasing. This observation is reflected in the demand for multiplexers which is expected to decline by 14% in 1997 following the 10% decline in 1996, while cell and frame relay equipments are projected to grow 100% in sales worldwide in 1997. And tonight (4 February 1997) an infoseek keyword search of "cryptography" turned up over 23,000 internet web site references. These somewhat random recollections are just a reflection of some recent reading and are intended to illustrate the exponential revolutionary changes taking place in the "world's largest machine".

(FOUO) The internal changes that we at NSA have witnessed as we face this revolution are profound. Think of how the blessing and curse of e-mail have changed your work in the past five years. There have been numerous organizational changes and consolidations. The astronomical number of working groups, focus groups, steering groups, tiger teams and efforts to "re-engineer" our business and its processes are efforts to correct our inability to change rapidly enough. Some changes do come quickly though. We are forming alliances with industry and foreign partners which just five years ago would have seemed inconceivable. Though the pace of restructuring and personnel moves designed to help us meet the challenges we face more effectively seems so rapid and at times unproductive, it is likely to continue and even increase.

(FOUO) The most important things that individuals can do to prosper in this environment is to acquire new skills and shed their "tribal loyalties". The ability to learn and "globalize" your role in the intelligence mission are the two most important things that you can do for your career, job satisfaction and ability to contribute meaningfully. Those who view themselves only as cryptanalysts or signals analysts or A,B,.,Z Groupers or mathematicians or engineers will have a very difficult time finding their niche. The future of NSA belongs to those who view themselves as "intelligence professionals". It belongs to those who identify with the production of both information security and SIGINT products and not solely any organizational unit or discipline. Our success will depend on these boundaries vanishing at the individual level.

(FOUO) In an environment where resources are diminishing and expectations are increasing, it is unlikely that any organizational unit will be able to accomplish its mission in isolation. The stovepipes are disappearing and projects that have participants from diverse organizations (across key components) are becoming commonplace. The reason for this is simple: duplicative efforts and overlapping missions are being eliminated and we are striving to get more from existing resources. One area in which this applies to Z Group is tools and techniques development. We are moving to an environment in which the tools and techniques which are developed for analysis will move directly into the production environment. That means that the software developed during analytic process will become an integral component of collection and processing systems developed outside of Z Group. A collection system tightly coupled with a networked "analysis web" and the industrialization of software production made possible by object-oriented

programming are the technologies that will enable such software reuse. Culturally analysts and developers may work in two different key components or even another agency during the course of a single project. Flexibility and loyalty to our customers will become far more important to success in our careers than organizational affiliation.

~~(FOUO)~~ The challenge of getting this machine to work for our nation's security appears daunting. We should remember that there are boundless opportunities made possible by the very same developments that appear to threaten our ability to deliver our customers the information products that they need. Our success in capitalizing on these opportunities will be reflected by our capacity for learning and ability to change.

2. (U) CALENDAR

Feb 5	Deadline for SCAMPS input (see 6a)
Feb 13	Scientific & Engineering Society Presentation (see 6b)
Feb 27 - 7 Mar	CLA Film Festival (see 6c)
Mar 10 - 14	[redacted] Lectures (see 6d)
PLAN AHEAD	
Apr	Call for Unclassified Math Papers (see 6e)
Apr 7 - 11	Signals Analysis & Development Conference (see 6f)
May 5-9	ACE '97 at CCR-Princeton
Oct 29-31	Seventh Symposium on Cryptologic History (see 6g)

(b)(3)-P.L. 86-36

3. (U) KRYPTOS News

3a. ~~(FOUO)~~ 1997 Officers and Committee Chairs

President
President-elect
Secretary
Treasurer
Member-at-Large/CACP Rep
Member-at-Large/
Member-at-Large
New Member-at-Large
New Member-at-Large
Membership
Crypto/Math Rep
Publicity
UKLO-3
BANCC Chair
Newsletter
Historian
Awards

[redacted]

[redacted]

Retired Members	[redacted]	963-1127	[redacted]
Programs			
Literature		963-1451	
CA Intern Rep		968-7051	

3b. (U) 1997 KRYPTOS MEMBERSHIP APPLICATION (b)(3)-P.L. 86-36

DUES: $5.00 (Annually)

MEMBERSHIP YEAR: 1997 ( ) NEW ( ) RENEWAL

NAME:_____ DATE: _____

SECURE PHONE: _____ NON-SECURE: _____

ORG: _____ BLDG: _____ ROOM NR. _____

SID & HOST: _____

INTERESTED IN CHAIRING A COMMITTEE? ____YES ____NO

INTERESTED IN WORKING ON A COMMITTEE? ____YES ____NO

CHECK COMMITTEES OF INTEREST TO YOU:

____ CRYPTANALYTIC LITERATURE ____ MEMBERSHIP

____ DISTINGUISHED MEMBERS ____ PUBLICITY ____AWARDS

____ PROGRAMS ____ NEWSLETTER ____ RETIRED MEMBERS

Please return to [redacted]

//

4. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS (b)(3)-P.L. 86-36

(U) CACP Announcements

~~(FOUO)~~ The CA Intern Panel welcomes its newest intern, [redacted] who was just hired by NSA in January.

//

5. (U) TECHNICAL ARTICLES

5a. ~~(FOUO)~~ "New Research Model in Z"
by [redacted]

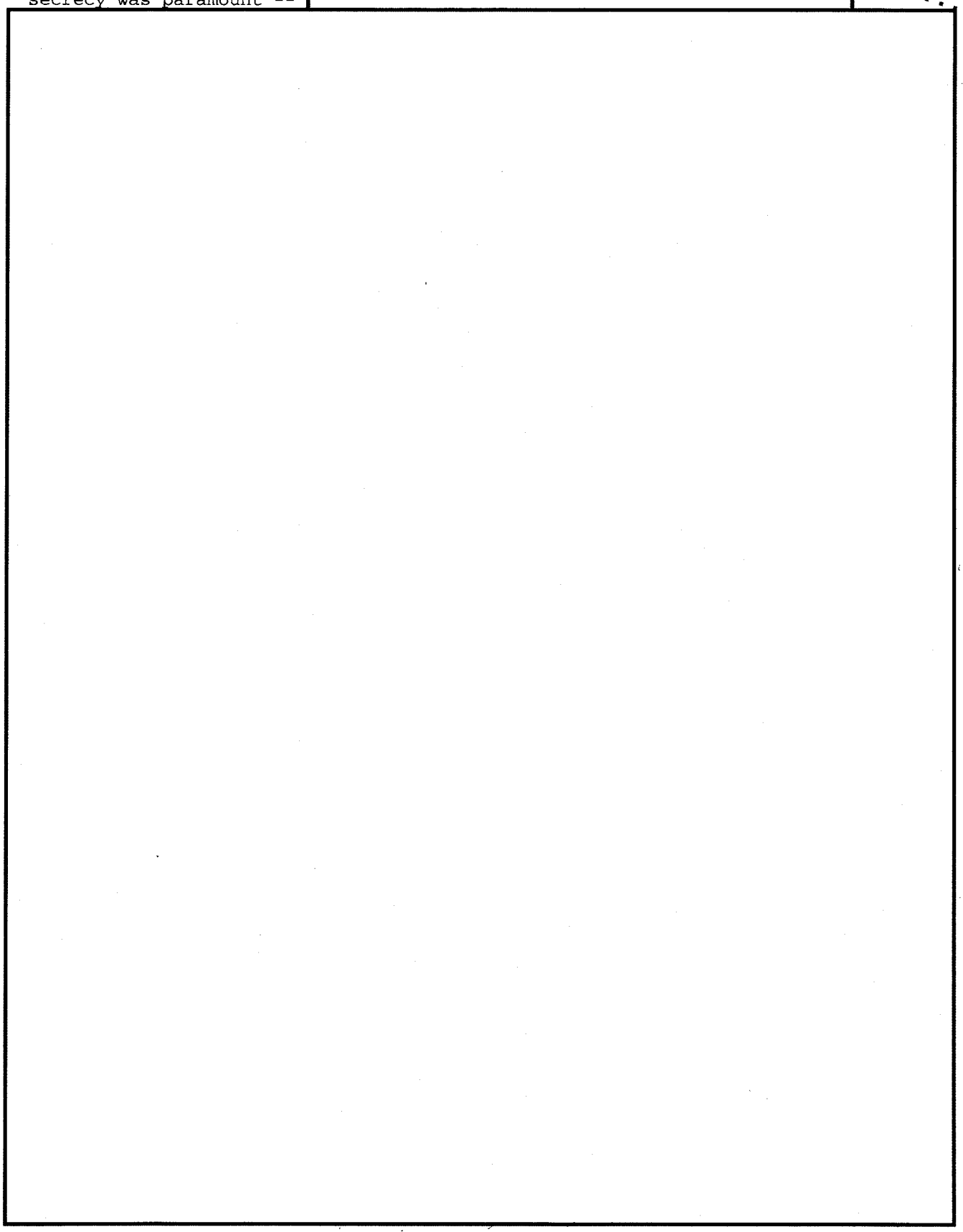
~~(TSC)~~ As we all have learned, the CA problem at NSA is changing profoundly. In the past and, to a large extent today, in a typical problem, some unsung hero (aka "the bit fairy") would provide data to the cryptanalyst who would practice his or her arcane art attempting to resolve some aspect of a cipher machine. Cryptanalysis, mathematics, and computing capability are three

(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

vital pillars to support the "arcane art". For success, the element of secrecy was paramount --



~~(S)~~ Are we going to have problems with this new method of research? Of course -- culture changes are always difficult. Line organizations will have difficulty sparing vital people to staff pods. One difficult management challenge will be to find the proper balance between short-term operation requirements and long-term research needs. In many instances there will be no clear-cut organization to support follow-on efforts. And many other problems must be apparent. However, this is now our model for performing research in Z Group and senior Z Group management is committed to it.

5b. (U) Matt on Math (b)(3)-P.L. 86-36
By: [redacted]

~~(FOUO)~~ "A Brief Introduction to Factoring, Part I"

(U) If you stop somebody in the hall and ask them "What is the prime factorization of 21?", chances are they will reply that 21 = 3 * 7. If we inquire as to how they discovered the factorization, it will undoubtedly be by trial division, unless that person is a number theorist. The point of this article is to introduce you to some interesting, non-intuitive ways for finding the prime factorization of a composite integer.

(U) Surprisingly, today's most powerful methods of factoring have their roots in elementary algebra. Suppose we wanted to factor a composite integer N into primes. If we could write N as a difference of perfect squares

$$N = a^2 - b^2$$

then we know that

$$N = (a + b) * (a - b)$$

and could easily recover the factors. For example, let N = 8051. Then

$$\begin{aligned} 8051 &= 8100 - 49 \\ &= 90^2 - 7^2 \\ &= (90 + 7) * (90 - 7) \\ &= 97 * 83. \end{aligned}$$

This idea is attributed to Pierre de Fermat. Furthermore, if N is odd, then this will always work! Unfortunately, finding the squares a and b is a difficult task.

(U) In the mid-1900s, Maurice Kraitchik refined Fermat's technique. Kraitchik realized that it is better to look for random (a,b) pairs such that

$$a^2 - b^2 = k * N$$

is some multiple of N. If k = 1, then we have the Fermat case. If, however, k =/= 1 then we know that N divides a^2 - b^2 so the greatest common divisor

(b)(3)-P.L. 86-36
[redacted]

Doc ID: 6823813

gcd(a + b, N)

might give us a non-trivial factor of N. We're not always that lucky, i.e. gcd(a + b, N) might be 1 or even N itself. In fact, this happens half of the time.

(U) How do we factor N = 689 using Kraitchik's ideas? The first square that exceeds N is 27^2 = 729. Starting with i = 27 and iterating, we see that f(i) = i^2 - N factors as

f(27) = 27^2 - 689 = 40 = 2^3 * 5

f(28) = 28^2 - 689 = 95 = 5 * 19

f(29) = 29^2 - 689 = 152 = 2^3 * 19.

Now, the product of these three easy factorizations gives us a congruence of squares modulo N!

$$\begin{aligned}(27 * 28 * 29)^2 &= 2^3 * 5 * 5 * 19 * 2^3 * 19 \\ &= 2^6 * 5^2 * 19^2 \\ &= (2^3 * 5 * 19)^2 \\ &= 760^2\end{aligned}$$

Finally we compute

gcd(27*28*29 + 760, 689) = 53

and so

689 = 13 * 53.

(U) This looks very simple. In reality, this very simple example wasn't easy to find. What we need is an algorithm for efficiently generating (a,b) pairs. The first to do this were John Brillhart and Michael Morrison. Their idea used only basic linear algebra. Let the "factor base" FB be the set consisting of the primes below 23

FB = { 2, 3, 5, 7, 11, 13, 17, 19 }.

We record the three difference of squares equations above by storing a vector of exponents, i.e.

v(27) = [3, 0, 1, 0, 0, 0, 0, 0]

v(28) = [0, 0, 1, 0, 0, 0, 0, 1]

v(29) = [3, 0, 0, 0, 0, 0, 0, 1].

Since, we're only interested in finding squares, it is sufficient to record the exponents modulo 2 (i.e. write a zero if the exponent is even and 1 otherwise):

v(27) = [1, 0, 1, 0, 0, 0, 0, 0]

v(28) = [0, 0, 1, 0, 0, 0, 0, 1]

v(29) = [1, 0, 0, 0, 0, 0, 0, 1].

(b)(3)-P.L. 86-36

Note that the sum (modulo 2) of these three vectors is the zero vector. This tells us that the product of 27, 28, and 29 is a square since all the exponents are even!

(U) To automate this on a computer, we would find (at least) 9 vector "relations" v(i) -- more relations then elements in the factor base. Once we have done this, we have (at least) 9 vectors in a 8-dimensional vector space. Linear algebra tells us that the vectors must be dependent. Since the v(i)'s are populated with zeros and ones, a linear dependence is precisely a subset of vectors that sum to the zero vector!

(U) In 1981, a refinement of the Brillhart-Morrison algorithm was announced by Carl Pomerance. The method is known as the quadratic sieve. The basic idea is to generate small quadratic residues modulo N using a technique similar to the sieve of Eratosthenes (used to quickly generate prime numbers). We save the residues that are divisible only by the primes contained in some factor base and call them "smooth". Once we've collected enough smooth residues, we use linear algebra (as above) to find a combination of that that is a square. Finally, we use the same gcd trick to (hopefully!) get a factor.

(U) Until recently, the quadratic sieve (and its variants) was the mainstay of the factoring community. In 1988, John Pollard introduced an idea that used algebraic number fields to factor certain large numbers like Mersenne numbers (2^N - 1). In 1990, a team led by Hendrik Lenstra factored the number 2^512 - 1 using Pollard's number field sieve.

(U) Even with this success, many believed that the number field sieve would be practical for "general" numbers. Where there is a will, there is a way. The collective work of many mathematicians produced a number field sieve for general numbers. This method was used by Arjen Lenstra to factor a 130-digit number that was the product of two large primes.

(U) Do we always want to use a method of factorization like the quadratic sieve? The answer is no. Methods like the quadratic and number field sieve split numbers N into two pieces. It wouldn't be nice to spend months worth of computer time with the number field sieve to find that

114267383931839306531511177430664118370566644248626910538120 99

= 13 * 878979876398763896396239826389723987465897263450976234908623.

Are there any slick ways to pull off small-ish factors of a number quickly? We'll see some in next month's article!

"""""""

researchers, and cleared academic consultants. These 12-week conferences are called SCAMP workshops. Many important cryptanalytic techniques and many breakthroughs on current mission-critical problems have come out of SCAMPs over the years.

(U) Topics for the three SCAMP conferences are taking shape now and it is time for Agency technical people to indicate their interest in attending a workshop. A brief description of each topic is given below. These conferences provide a great career development opportunity. Current plans are to send 5 people to Princeton, 5 to La Jolla, and a relatively large group to Bowie.

(U) If you are interested in attending a SCAMP please talk to your local management and make sure that your name gets to me as well. We need to hear >from you by 5 February 1997. Shortly after that the selection committee will meet.

[redacted] R51

(b)(3)-P.L. 86-36

////////////////////////////////////

~~(FOUO)~~ SCAMP AT IDA-CCR PRINCETON

(U) "Mathematical Methods for Data Modelling and Filtering"

~~(S)~~ The goal of this SCAMP is to [redacted]

[redacted] So the subtext for this SCAMP might be "Spreading the Mathematical Gospel".

(b)(1)
(b)(3)-P.L. 86-36

~~(FOUO)~~ [redacted] have agreed to serve as co-chairs.

////////////////////////////////////

~~(FOUO)~~ SCAMP AT IDA-CCR LA JOLLA

~~(TSC)~~ Our SCAMP this coming summer will focus on [redacted]

[redacted] This is a good example of new challenges stemming >from a changing worldwide communications environment.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

////////////////////////////////////

~~(FOUO)~~ SCAMP AT IDA-CCS BOWIE:

~~(TSC)~~ The 1997 SCAMP at IDA CCS will study [redacted]

[redacted]

(b)(3)-P.L. 86-36

[redacted]

6b. (U) Science and Engineering Society Presentation

(FOUO) THE SCIENCE AND ENGINEERING SOCIETY

presents
DR. MATT BLAZE
(He found the weakness in the CLIPPER chip)
AT&T LABS
speaking on

"TRUST MANAGEMENT: CERTIFICATES AS PROGRAMS"

FEBRUARY 13 1996
10:00 AM
R&E SYMPOSIUM CENTER

(U) Abstract: We identify the "trust management problem" as a distinct and important component of security in network services. Aspects of the trust management problem include formulating security policies and security credentials, determining whether particular sets of credentials satisfy the relevant policies, and deferring trust to third parties. Existing systems that support security in networked applications, including X.509 and PGP, address only narrow subsets of the overall trust management problem and often do so in a manner that is appropriate to only one application. This talk presents a new approach to trust management, based on a simple language for specifying trusted actions and trust relationships in certificates and policies. We will also describe a prototype implementation of a new "trust management system," called PolicyMaker, that will facilitate the development of security features in a wide range of network services.

~~(FOUO)~~ Bio: Matt Blaze is a Principal Research Scientist at AT&T Laboratories, and an adjunct Professor of Computer Science at Columbia University. His primary research areas include computer security, applied cryptology, and large scale distributed computing systems. His recent work has been influential in shaping the technological aspects of US cryptography policy; his 1994 discovery of a weakness in the US Government's proposed CLIPPER key escrow system was a turning point in the cryptography debate and has sparked an ongoing area of cryptography research. His current interests focus on the use of secure hardware, the management and specification of trust, public key certificate infrastructure, and cryptography policy. Dr. Blaze holds a Ph.d. in Computer Science from Princeton University, an MS from Columbia University, and a BS from the City University of New York. He received the Electronic Frontier Foundation's Pioneer award in 1996. He serves as a member of the Federal Networking Council Advisory Committee.

~~(FOUO)~~ This presentation is scheduled to be broadcast on Channel 17. For membership in or information on the Science and Engineering Society contact Tom Kline [redacted]

THIS PRESENTATION IS OPEN TO ALL PERSONNEL

6c. ~~(FOUO)~~ CLA Foreign Film Festival (b)(3)-P.L. 86-36

~~(FOUO)~~ "Famous Actors Week" 27 Feb - 7 Mar 97

The Crypto-Linguistic Association (CLA) Foreign Film Committee will

[redacted]

present a program of four foreign language films featuring well-known actors. Here's the schedule for Famous Actors Week:

"Pelle the Conqueror" (Danish, 138 min):	Thu., 27 Feb	1100-1330
	Fri., 28 Feb	" "
"A Rhapsody in August" (Japanese, 98 min):	Mon., 3 Mar	1100-1245
"Mississippi Mermaid" (French, 110 min):	Tue., 4 Mar	1100-1300
"M" (German, 99 min):	Wed., 5 Mar	1100-1245
"A Rhapsody in August" (Japanese, 98 min):	Thu., 6 Mar	1100-1245
"Mississippi Mermaid" (French, 110 min):	Fri., 7 Mar	0900-1100
"M" (German, 99 min):	Fri., 7 Mar	1300-1445

(U) First there was "Pelle the Conqueror" and then there was "Conan the Barbarian". Our film, however, is hardly about barbarian conquest and stars German actor Max von Sydow speaking Danish.

(U) "A Rhapsody in August" features Richard Gere speaking a fair amount of Japanese (from what we've been told) and this is NOT a dubbed movie. Come and find out how good his Japanese is!

(U) "M". They don't make them like this anymore! CLA picked that master of the early horror flick, British actor Peter Lorre (speaking German), in this 1931 thriller.

(U) "Mississippi Mermaid" starring Catherine Deneuve and Jean Paul Belmondo apparently has nothing to do with neither the Magnolia State, the muddy Mississippi, nor with underwater beauties. Come and see what it's about!

~~(FOUO)~~ All films will be shown in OPS2B4118 Room #2 (seats: 30). Bring your lunch as it's lunchtime for most of us. YOU DON'T HAVE TO BE A CLA MEMBER TO ATTEND.

[redacted]
CLA Foreign Language Film Committee Chairman

6d.(U) CMI Sponsored Guest Lecture

~~(FOUO)~~ [redacted] LECTURES 10-14 MARCH FANX II 1300-1500

~~(FOUO)~~ [redacted] renowned cryptanalyst, mathematician, lecturer, and author, who has successfully worked on a number of very important Agency problems and has played a critical role in the discovery and development of many of the most important cryptanalytic techniques, will give a one-week series of lectures from 10 to 14 March. The lectures will be held in the FANX II auditorium from 1300 to 1500. The first four talks will be based on four major cryptanalytic problems and the techniques that came from their analysis. The fifth is on unsolved problems.

(b)(3)-P.L. 86-36

6e.(U) CALL FOR UNCLASSIFIED MATHEMATICS PAPERS

(U) NSA Mathematicians:

You are invited to submit any unclassified mathematics papers you have written in recent years to be considered for inclusion in a collection of unclassified papers that we are putting together for recruitment purposes.

[redacted]

The papers should have some relevance to our work at the Agency and be at most 15 pages or so in length. Papers that have appeared in journals are excellent candidates for this collection, but that is not a requirement. (In the case of papers that have appeared in journals we will just photocopy the journal version so it will be easy.)

[redacted] will make the selections and edit the collection. If you would like to contribute a paper, please forward it to Bob in R51.

If you have a paper in progress give Bob a call and talk about it. We would like to send the job to the printers by May 1, so you really have to get in the game by sometime in April at the very latest.

[redacted] R51

(b)(3)-P.L. 86-36

6f. ~~(SC)~~ 1997 Signals Analysis & Development Conference

~~(SC)~~ IRT below message, the 1997 Signals Analysis and Development Conference, sponsored by Z6, will be held 7-11 April. We have demos, focus sessions, and presentations planned! Would you like to attend and take part in what promises to be an exciting conference? We have room for more demos and presentations. Please read below message and contact me by 14 Feb if you are interested in attending/participating. Look forward to hearing from you.

[redacted] Conference Leader, [redacted]

~~(FOUO)~~ Formal message, [redacted] DTG 311550Z Jan 97

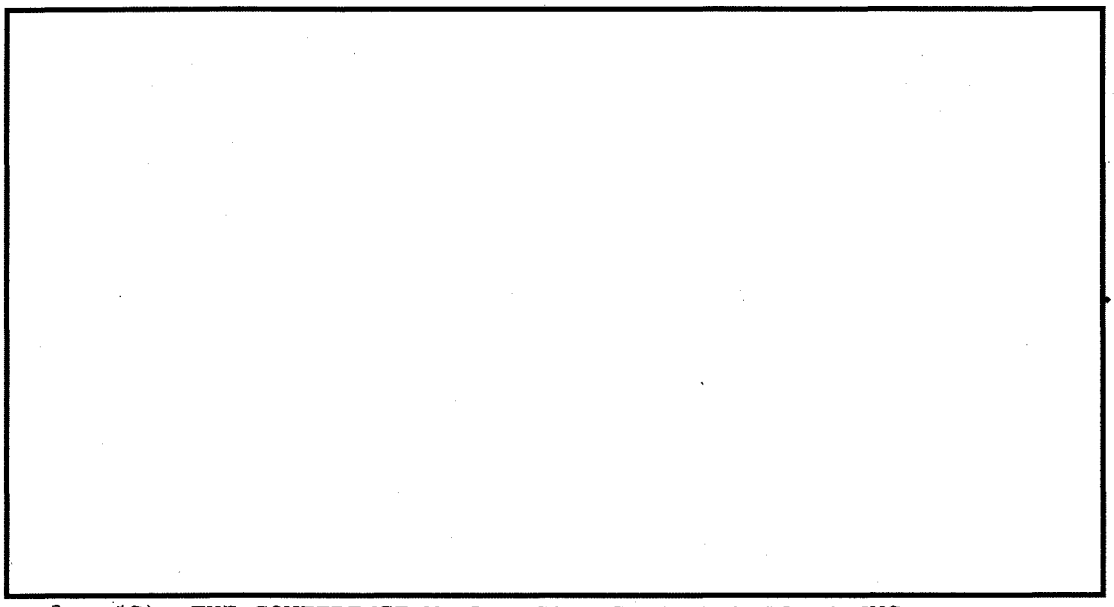
(U) SUBJECT: 1997 SIGNALS ANALYSIS AND DEVELOPMENT CONFERENCE: CALL FOR PARTICIPATION AND PRESENTATION BY 14 FEB 97

1. ~~(S-CCO)~~ THIS MESSAGE ANNOUNCES THE FIFTH ANNUAL SIGNALS ANALYSIS AND DEVELOPMENT CONFERENCE, SPONSORED BY Z6, THE OFFICE OF SIGNALS ANALYSIS AND DEVELOPMENT. THIS YEAR'S CONFERENCE, TO BE HELD THE WEEK OF 7 - 11 APRIL, WILL BE DIFFERENT FROM RECENT YEARS, AND, WE FEEL, EXTREMELY EXCITING!! WE ARE PLANNING A CONFERENCE THAT WILL RESEMBLE THE W3 SEARCH CONFERENCES OF OLD, BUT WILL ALSO COMBINE SOME FEATURES FROM PREVIOUS SYMPOSIUMS AND DATA DEMOD WORKSHOPS. THE 1997 SIGNALS ANALYSIS AND DEVELOPMENT CONFERENCE HAS ADOPTED THE THEME "THE TECHNOLOGY OF SIGNALS ANALYSIS". THE WEEK WILL BE FILLED WITH PLENARY BRIEFINGS AND LOTS OF DISCUSSIONS AND WORKING GROUP SESSIONS. THE Z6 LEADERSHIP TEAM, BOTH MANAGERIAL AND TECHNICAL, IS COMMITTED TO MAKING THIS YEAR'S CONFERENCE ONE WHERE WE CAN SOLVE PROBLEMS AND BUILD LASTING RELATIONSHIPS. THROUGH THIS COMMITMENT WE FEEL THAT THE SIGNALS ANALYSIS COMMUNITY WILL STAY FOCUSED ON THE COMPLEX TECHNOLOGIES WE ARE FACING TODAY AND THOSE WE WILL FACE AS WE ENTER THE 21ST CENTURY.
2. ~~(SC)~~ THIS YEAR'S CONFERENCE WILL FOCUS ON THE FOLLOWING SPECIFIC SUBJECTS/TOPIC AREAS:
A) THE ANALYSIS WEB
B) NEWEST TECHNOLOGIES, SUCH AS [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

- COMPUTER-TO-COMPUTER CHALLENGES

[redacted] (b)(3)-P.L. 86-36



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

3. ~~(S)~~ THE CONFERENCE WILL ALSO INCLUDE THE FOLLOWING:
A) WELCOME BREAKFAST FOR ATTENDEES (COST: $6 - $7 PER PERSON),
B) VENDOR DAYS, WHERE SEVERAL LOCAL TECHNOLOGY VENDORS WILL BE INVITED TO SHOW THE LATEST IN TOOLS AND EQUIPMENT,
C) FOCUS SESSIONS FOR ABOVE TOPICS (WE WILL NEED MENTORS FROM BOTH HERE AT NSA, AS WELL AS FROM VISITING LOCATIONS),
D) NUMEROUS DEMOS OF THE LATEST SIGNAL ANALYTIC TOOLS, BOTH SOFTWARE AND HARDWARE, AS WELL AS A
E) HAPPY HOUR AT A LOCAL ESTABLISHMENT.
4. ~~(S-CCO)~~ PLEASE FORWARD THE FOLLOWING INFORMATION NLT 14 FEBRUARY 1997:
A) NAMES OF PROPOSED ATTENDEES, EMAIL ADDRESS AND SECURE PHONE
B) IF YOU WOULD LIKE TO PRESENT A BRIEFING OR DEMONSTRATION, FORWARD SUGGESTED PRESENTATION TITLE, SHORT ABSTRACT, CLASSIFICATION AND TIME REQUIREMENT
- BRIEFINGS MUST RELATE TO TOPICS IN PARA 2 ABOVE
  -- ALL SUGGESTED PRESENTATIONS WILL BE REVIEWED FOR RELEVANCY
  -- Z6 WILL LIMIT THE NUMBER OF PRESENTATIONS DUE TO THE LARGE NUMBER OF DEMOS AND WORKING SESSIONS PLANNED
  -- SITE OVERVIEW BRIEFINGS ARE DISCOURAGED
- DO NOT EXCEED THE CLASSIFICATION LEVEL OF TOP SECRET CODEWORD AND DO NOT CONTAIN "NOFORN" OR "NOCONTRACT" INFORMATION.

C) FORWARD TOPICS NOT MENTIONED IN PARA 2 THAT WOULD BENEFIT SITE SIGNALS ANALYSTS (E.G., SPECIFIC SOFTWARE/HARDWARE TRAINING).
D) INDICATE IF YOU WILL ATTEND THE OPENING BREAKFAST (OPENING REMARKS AND WELCOME PACKAGE DISTRIBUTION ARE PLANNED AND ARE AN IMPORTANT PART OF THE CONFERENCE).
5. ~~(C-CCO)~~ A TENTATIVE CONFERENCE AGENDA, AND CLEARANCE AND BRIEFING REQUIREMENTS WILL BE PREPARED AND TRANSMITTED AFTER RESPONSES FROM OUR COLLEAGUES AT UK/GCHQ, AUS/DSD, CAN/CSE, NZ/GCSB, FIELD SITES AND NSA HQS HAVE BEEN RECEIVED.
6. ~~(C-CCO)~~ QUESTIONS MAY BE DIRECTED TO [redacted] CONFERENCE LEADER, VIA EMAIL [redacted] OR PHONE, [redacted] (SECURE)/ [redacted] PLEASE INCLUDE [redacted] ON ALL EMAIL MESSAGES. TO ENSURE YOU HAVE THE MOST CURRENT INFORMATION ON CONFERENCE PLANNING, PLEASE REFER TO OUR HOME PAGE ON NSA'S WEBWORLD [redacted]. THE URL

(b)(3)-P.L. 86-36

[redacted]

IS IN LOWER CASE WITH THE EXCEPTION OF [redacted] WITH THE CONFERENCE FAST APPROACHING, IT IS IMPERATIVE THAT YOU RESPOND BY 14 FEB 97.

....

6g.(U) CALL FOR PAPERS: Seventh Symposium on Cryptologic History

(U) Seventh Symposium on Cryptologic History

29, 30, and 31 October 1997

The National Security Agency

will sponsor and host

the seventh Symposium on Cryptologic History,

29 to 31 October 1997 at NSA,

Ft. George G. Meade, Maryland.

(U) The conference will focus on cryptologic history based on recently declassified materials from World War II and the VENONA releases.

(U) The Center for Cryptologic History welcomes papers and panels relating to any aspect of cryptologic history based on research into declassified materials.

(U) To propose either a complete session or individual paper you should submit:

a) a one page abstract for each paper
b) a one page statement of session purpose for a panel; and
c) a brief vita for each presenter to:

Dr. David A. Hatch, Chief
Center for Cryptologic History (S542)
National Security Agency
9800 Savage Road, STE6886
Fort George G. Meade, MD 20755-6886

Telephone: [redacted]

Deadline for submission is 1 April 1997

(U) Information about registration, accommodations, and program will follow in June 1997.

(b)(3)-P.L. 86-36

....

//////////

8. Problems and Puzzles by [redacted]

(b)(3)-P.L. 86-36

8a.(U) Answers to Kristmas Kryptos Kwiz!

(FOUO) This year we saw an increase in the number of entrants, and the resulting scores. Top honors go to the team of [redacted] with an astounding score of 88! Second place goes to the team of [redacted] with 73,

[redacted]

and [redacted] came in third with 68. Other solutions were submitted

(U) Congratulations to all those that entered! (b)(3)-P.L. 86-36

(FOUO) The answers to the quiz follow. Question 10 was thrown out. If anyone needs another copy of the questions, e-mail me at [redacted] Be aware that several questions can have more than one correct answer.

1. Between "hand" and "dark". The list comprises five sets of ten words: the words are sorted according to a word associated with each of the listed words. The five sets are phrases (a) beginning with a country (b) beginning with a colour (c) beginning with a part of the body (d) beginning with an ordinal and (e) of the form xxxx in the xxxx.

Afghan hound	black art	blue blood	brown bread
chin strap	Chinese lantern	Cuban heel	Danish pastry
dog/manger	drop/bucket	dyed/wool	ear wig
elbow grease	fifth column	first class	fly/ointment
foot soldier	fourth dimension	French leave	green belt
grey matter	hand shake	hip flask	Indian summer
jack/box	knee cap	Maltese cross	man/moon
nineteenth hole	Norwegian wood	nose bag	orange peel
pain/neck	pie/sky	pink gin	red brick
second hand	seventh heaven	shot/dark	shoulder blade
sixth sense	Spanish fly	Swiss roll	third world
toad/hole	twelfth night	twentieth century	white collar
wrist watch	yellow pages		

2. DISCOVER HANGOVER BROWSING SONGBIRD BATHROOM SOMEWHAT EVERMORE OVERHEAD
LANDRAIL HEADNOTE BOOKWORM WOODWARD SHIPYARD LANDLORD KINSFOLK LANDWARD

3. light, work, long, land, stone, man, band, on;
head

4. 5. [over x] [equals +] [times -] [minus /] [plus =]
thus 2 + 6 / 4 = 3 - 1; 4 x 7 - 3 / 5 = 5

1 + 1 - 1 x 1 / 1 = 1

5. ZBYWZ. Viewed from afar, the tape spells out KRYPTOS KRISTMAS KWI, which is completed by OOOOO or ZBYWZ.

```
  O
 O
O
OOOOO
```

6. All are based on Roman numerals
(a) 300 (CCC - symmetry)
(b) 59 (LIX - 3 Roman numerals)
(c) 57 (LVII - 4 Roman numerals)
(d) 111 (CXI - same numbers of digits and Roman numerals)

7. (a) ZAP (BAP.....TAP) - 11 words
(b) CLICKING (CLOCKING....CLACKING) - 4 words.

(b)(3)-P.L. 86-36

[redacted]

8. 3.41 (=2 + Sqr(2)) inches

9. (a) MICHELANGELO (b) PIERRE FERMAT (3rd 4th and 5th letters of each word)
10. Orchestras. THIS QUESTION CANCELLED

11. (a) FRED MESSAGE RECEIVED AND UNDERSTOOD STOP JOE X
(b) He mistyped the first letter of his name (G instead of F). As the message indicated, K(n) + K(n + 1) = K(n + l) where l is the length of the secret key - in this case 10 (FREDBLOGGS).

12. (a) 105 (previous number plus the number of letters in its name)
(b) 14 (N minus the number of letters in N)
(c) 11 (N minus the number of letters in N+1)
(d) 26 (N plus the number of letters in N)
(e) 52 (values which can be expressed as the sum of two squares)
(f) 4181 (alternating values of the series 1 1 2 3 5 8 13 21...)
(g) 6 (lengths of the names of the months)
(h) 122 (dates of first Monday in each month of 1996 - month/day)

13. In how many ways can you put n letters into n envelopes (one letter in each envelope) such that no letter is in the correct envelope? The answer is the nearest digit to n!/e.

14. 4:1

15. (a) NITROGEN (not one of the inert gases)
(b) TIGER (not native to Africa)
(c) POLANSKI (not American)
(d) BRASILIA (not in Northern hemisphere)
(e) MORPHEUS (a God, not a Goddess)
(f) FLANDERS (a WWII battle, not WWI)
(g) COLUMBIA (others have unique languages)
(h) TIGER (not 8 letters long)

16. Blue. The list is ALPHA BRAVO CHARLIE ... ZULU. 25 21 is "YANKEE UNIFORM".

17. (a) MEIOSIS (or LITOTES) (b) HYPERBOLE (c) TMESIS

18. (a) George Orwell (1984 = 31 x 64)
(b) Stanley Kubrick (2001 = 3 x 23 x 29)

19. Alias SMITH and JONES! In order, Inigo J, Capt John S, Bessie S, Jennifer J, Maggie S, James Earl J, Tom J, Ian Crichton S, Calvin S.

20. (a) Doris Day (b) Woody Allen (c) Lewis Carroll
(d) Fred Astaire (e) Moliere (f) George Sand

21. Each name is an anagram of another name.

22. CANAL + RACES = TAPED

23. (a) ROBINSON CRUSOE (b) A FAREWELL TO ARMS (c) SONS AND LOVERS
(d) ONE DAY IN THE LIFE OF IVAN DENISOVICH

24. 19 (Countries embedded backwards in the text. Note that SOMALIA contains MALI.)

25. 21. With the alphabet YAOESP-IRTBLV-H-WDCFKM-GN, one can form the words RASE/SEAR, TARO/ROTA, BAAS, LYRE/RELY, OPTS, HAVE, WARP, CODE/DECO,

FADS, ZEBU, SIMA, KEPI/PIKE, MERI/RIME, BIGA and WINS.

26. (a) North/south of the equator (b) Number of syllables
(c) Number of land borders (d) Length of name of capital
(e) Population less/more than 50m
(f) difference in length between the country name and the adjective derived from it

27. Either PANAMA MADAGASCAR ARGENTINA NAURU RUSSIA or
PANAMA MALTA TAJIKISTAN ANGOLA LAOS/LATVIA

28. Ada, Anna and Anne Dean (nee Dene); add Dan, Dean, Den (dead) and Ed, and end Dad and Nanna (addenda) - an ennead, and a dead end!

29. (a) OPST (SPOT TOPS OPTS POST)
(b) ADEEGNR (GRENADE ANGERED ENRAGED GRANDEE)
(c) AACEINRST (ASCERTAIN SECTARIAN CARTESIAN)
(d) AEIGNRT (ALERTING ALTERING INTEGRAL RELATING TRIANGLE)
(e) EILOSTT (LITOTES T S ELIOT TOILETS)
(f) ABDELM (BEDLAM BLAMED AMBLED)

30. (a) (A)LIEN
(b) CAME(O)
(c) P(I)LEA

31. ARE(A)

32. LONDRES. (The languages must be represented by the word for each in its natural tongue - SUOMI for FINNISH etc).

33.
```
180 = (3 x 5!)/(5 - 3)        181 = (35 x 5) + 3!
182 = (5! x .5r -3!) x 3      183 = 5!/.5r - 33
184 = 3!!/5 + 5!/3            185 = 5 x (5!/3 - 3)
186 = 5! + 33/.5              187 = 3/(.5**3!) - 5
188 = (5 - .3) x 5!/3         189 = 5!/.5r - 3**3
```

34. PARTY. The text is "THE QUICK BROWN FOX..." and the message is "NOW IS THE TIME..."

35. MERRY CHRISTMAS (last two columns (boustrephedon) when ARMS IDEA HARM PORT SAYS VICI RUHR are written one under the other).

"""""""

*) Infinitely smart
*) Bloodthirsty
*) Greedy
Beginning with Pirate 5, they each make a proposal on how to split up the treasure. This proposal is either accepted or the pirate is thrown overboard. A proposal is accepted if and only if a majority of the pirates agrees on it. (All pirates vote on a proposal, including the one who makes it. A majority is more than half - thus, if there are two pirates and the vote is 1-1, someone gets thrown overboard. A pirate would rather get zero coins than get thrown overboard.)

(U) What proposal should Pirate 5 make?

"""
##

9.(U) EDITORIAL CORNER

REMINDER: Submissions for the March issue are due by February 25th.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

(~~FOUO~~) EDITORIAL BOARD

[redacted]
Jack Ingram, Cryptologic History Museum, [redacted]

(b) (3) -P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

[redacted]

TOP SECRET//COMINT

(b)(3)-P.L. 86-36

[redacted]

(U) [redacted] info
(U) Last Modified: 10/30/2002 11:42:22
(U)PE EXTERNAL PAGE

(b) (3)-P.L. 86-36

```
**************************************
*        TALES OF THE KRYPT          *
**************************************
                March 1997

////////////////////////////////////////////////////////////////////////////
****************************************************************************

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
////////////////////////////////////////////////////////////////////////////
```

(FOUO) TABLE OF CONTENTS:

1. Perspective

2. Calendar of Events

3. KRYPTOS News

4. Word from the CACP

5. Technical Article

6. Community Service

7. Problems and Puzzles

//

1. (FOUO) PERSPECTIVES - Each month this newsletter features the perspective of a Senior on a topic of his/her choice. This month we are pleased to publish the text of the address made by [redacted] Chair of the Cryptanalysis Career Panel, at the Breakfast Affair for Newly Certified Cryptanalysts (BANCC) on 29 January 1997.

~~~~~~

"Cryptanalysis Today" (FOUO)

(FOUO) It is a pleasure for me to participate in honoring our newly certified cryptanalysts. In doing that I would like to say a few things about Cryptanalysis in general and some things I see going on in our career field.

(FOUO) There is certainly a great deal of flux (uncertainty) in Cryptanalysis. There are a number of reasons for this:

- part of it is technology -- the ease with which unsophisticated targets can make quite sophisticated upgrades to the communications very quickly, cheaply, and I would say sometimes mindlessly (they don't have to be cryptographic experts to bring about these upgrades)

- part of it is the instability of the target set

- part of it is the fact that the volume of data we choose to handle (and I say "choose" deliberately because it's inarguable that we MUST stop doing some things and we don't do that well yet, certainly not in a globally organized fashion) --- the volume of data we choose to deal with keeps going up while our human resources go down [redacted]

(b) (3)-P.L. 86-36

- part of it is the floor shifting under our feet (organizationally; resource-wise; the tasks we are being asked to do; . . .)

(FOUO) That final factor is, I believe, a symptom of an organization coping with the other elements of change. Some might be inclined to wait until things calm down. That's a mistake. I don't think that we are going to see a "steady state" anytime soon. Quite the contrary, and so our outlook should be such that the structures we develop and, on a personal level, the mindset we take on should be ones that expect the dynamic condition to continue and that remain strong in that environment. It is like having a well-diversified financial portfolio that is not rocked by the changing economic winds. The fluidness and the uncertainty will continue. So what do we do? I remember that (prior to the formation of Z) G4 would put money in the budget for Special Purpose Devices to be developed 4-5 years down the line. The understandable question from the budget people was, "What do you want them to do?" The true answer was "Well, we don't know for certain but we know that we will need the SPDs and we know that, when the time comes, we WILL know what they are to do." As unsatisfying as that answer may seem (I don't think we were quite that blatant), those SPDs have, time and again, provided vital capabilities against important targets.

(FOUO) We find ourselves in a similar situation people-wise. We could ask, "What CA problems will we need to solve (in this environment where we make hard right turns, or our targets do, or technology does, . . .)?" Well, we don't know exactly but we DO know that

if we have cryptanalysts that TEAM well together,

if we have cryptanalysts with strong Leadership skills on those teams and in attacking CA problems in general,

if our cryptanalysts have a drive to stay on top of technology

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704
~~~~~~

and continue to learn throughout their careers,

if our cryptanalysts give back to the community and watch over its health and, in particular, the development of its new people, and

if we continue to instill in our cryppies the hunger for plain text that is our heritage,

THEN we will be as well-positioned as possible to resolve whatever CA challenges we encounter.

(TOUO) And so that message goes out -- repeatedly. It is reflected in advice that comes back from promotion boards ("We're looking for people with these qualities..."). It is reflected in the criteria for the Tech Track -- that the people we call "members" and "seniors" and "masters" have these credentials. It is the reason that mechanisms such as the Career Development Process exist, namely to create opportunities so that the desired skills can be developed and experiences obtained.

(TOUO) I know some people say that all of this smacks of pushing everyone to be a generalist, so I would like to put one caveat on the call for breadth and diversity that we hear so often, in the form of a story I heard in church over the weekend. It is the story of a young boy walking down the street carrying a ball and bat. He says to himself, "I am the greatest batter in the world." He throws the ball up, takes a mighty swing, ...and misses. Undaunted, he says again, "I AM the greatest batter in the world". He increases his focus, throws the ball up, takes a big swing, ...and misses. Feeling a little uncertain, he says again, in part to convince himself, "I am the greatest batter in the world." He focuses as never before, throws the ball up, swings, ...and misses. Crestfallen, shoulders drooping, head bowed, he's thinking despairingly, "What can I do now?" Suddenly, he picks his head up, looks up to heaven, gains new inspiration and encouragement, and says, "Wait a minute! I'm the greatest PITCHER in the world!"

(TOUO) We need pitchers ... and batters ... and fielders, coaches, ... and, yes, we even need managers. It is important to have some people who are well-versed across the board. It is also important to have people who are truly expert in given areas. So it is not wrong to find that niche and blossom there. Where we run into problems, where we become less effective as cryptanalysts is when we become isolated from and oblivious to the other parts of CA, the other capabilities, the other possibilities for attacking our targets. And thus the repetitive call to go learn about those possibilities. It is a call that cryptanalysts and supervisors should work in partnership to respond to (in some orderly fashion). It is for the good of everybody, certainly good for our technical health (individually and corporately) but also good for the career enhancement of the cryptanalyst (read: promotability & availability for certain jobs).

(TOUO) Those of you whom we are honoring this morning have demonstrated that you have taken substantive steps in this direction. In doing so you have opened doors (such as access to the TT) that will facilitate your further development. You have also (of interest to me as career panel chair!) positioned yourself to be called on for increased service to the CA community. For all of this, I congratulate you; I thank you in advance for your increased involvement; and, on behalf of the all the cryppies here, let me close by simply saying how pleased and proud we are to have you as colleagues.

---

2. (U) CALENDAR

This calendar is [redacted]

Mar 10 - 14	1300-1500, [redacted]	Lectures: "The Development of Machine Cryptanalysis and IDA's Involvement", FANX II
Mar 26	1315, KRYPTOS, [redacted]	"The Terrorist's Letter", Friedman Auditorium
Mar 17 - 21	CARD, GCHQ	
Mar 31	1300-1500, [redacted]	"The Math Community Town Meeting", R&E Symposium
PLAN AHEAD		
Apr 7 - 11	Signals Analysis & Development Conference, NSA	
Apr 21 - 9 May	IR-127, History of American Cryptology, FANX II CY-500 Course Center	
Apr 23-24	CA Conference: "The Changing Face of Cryptanalysis", IDA-CCS, Bowie	
May 5-9	ACE '97 at CCR-Princeton	
Oct 29-31	Seventh Symposium on Cryptologic History	

(b)(3)-P.L. 86-36

---

3. (U) KRYPTOS SOCIETY NEWS

3a. (U) KRYPTOS Society Meeting

[redacted]

(FOUO) KRYPTOS Program: "The Terrorist's Letter"

Presentation by [redacted]

Wednesday, March 26 at 1315

Friedman Auditorium

3b. (U) Apples for the Students

This article is UNCLASSIFIED in entirety.

The Giant Apples for the Students project is almost over for this year. The blue receipts indicate that there are only two weeks left (and those tapes are worth double the points!)

If you have been collecting for either of the two CMI-sponsored schools please send whatever you have now to either [redacted] or [redacted] is collecting for the Ruth Parker Eason School in Anne Arundel County which serves mentally and physically handicapped kids of all ages. Bob is collecting for the Immaculate Conception School in D.C. which provides challenging educational opportunities to underprivileged children of any faith. Please send in your reciepts as soon as possible so that [redacted] and Bob can meet the end-of-month deadline in getting them to the schools.

(b)(3)-P.L. 86-36

//

4. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

4a. (FOUO) NEW CA CERTIFICATION

(FOUO) Congratulations to [redacted] who was professionalized in CA this month!

4b. (FOUO) ANNOUNCEMENT OF 1997 CRYPTANALYSIS CONFERENCE:
"THE CHANGING FACE OF CRYPTANALYSIS"
APRIL 23-24 1997 -- IDA-CCS, BOWIE MD

(C-CCO) The Cryptanalysis Career Panel (CACP) is pleased to announce plans for a two-day, community-wide conference on the topic of "The Changing Face of Cryptanalysis", to be held on 23-24 April 1997 at IDA-CCS.

(C-CCO) For most of the conference, we will be examining three topics of emerging interest and growing importance to both the CA community and the larger NSA technical community. These topics include: protection and exploitation of computer networks and network-based communications systems; software and hardware reverse-engineering; and signals analysis. Each subject will be treated in the form of several presentations and a round-table, which will discuss approaches, progress, roadblocks, and future opportunities as seen from the perspectives of the diverse offensive and defensive missions for which the NSA technical community is responsible. In addition, part of the conference will focus on infrastructure issues of particular importance to cryptanalysts and CA aspirants, such as tech track, professionalization, and successful practices and processes in the CA workplace.

(b)(1)
(b)(3)-P.L. 86-36

(C-CCO) We hope to attract participants from across NSA's extended cryptanalytic and technical communities: [redacted] -- or use cryptanalytic tools and skills, regardless of an individual's occupational title, professional identity, or organizational affiliation. This cross-section of the community will include interns, trainees, SLEs, seasoned technical staff, and managers of technical areas.

(C-CCO) "The Changing Face of Cryptanalysis" conference will be a combination of technical awareness briefings, a comparison of notes on the best tools and methodologies for understanding and analyzing complex communications systems, and an opportunity for technical problem-solvers to strengthen their corporate identity and to make connections with other experts working elsewhere at NSA. The conference will not turn a newbie into a subject-matter expert. However, it should help to form connections between analysts with a solid grounding in CA tools, knowledge, and skills, and individuals involved with emerging or unconventional programs and technology. Building these bridges is of keen interest to the CACP, as the resulting connections will be essential for preserving the good health of NSA's core technical competencies as applied to problems of the future and for maximizing the effectiveness and productivity of its core asset: the individuals who comprise NSA's technical community.

(C-CCO) The CACP seeks your interest, participation, and involvement in this conference. Registration will be by self-nomination and will occur in the first half of March 1997; a conference announcement and registration procedures will be distributed very soon via email. The CACP will seek to ensure the participation of a broad cross-section of the NSA technical community.

(b)(3)-P.L. 86-36

[redacted]

4c. (FOUO) CAPQE

(FOUO) The CA PQE will be held on May 6 & 7 this year. The format for the PQE is a two-day, four-hours-per-day written test with eight questions presented each day. The aspirant's final score for the exam will be the total number of questions answered correctly over the two days. The passing score will be determined before the exam begins by an expert panel of cryptanalysts. Eligible aspirants who wish to take this exam must register in the panel office between 3 March and 12 April 1997. Review packets will be available at that time. PQE review sessions will be held during the month of April, and will be scheduled during lunch hours so as not to interfere inordinately with office work time. It is strongly suggested that aspirants prepare for these sessions by working the questions from the previous examinations. Since some of the review sessions will be held in small conference rooms, only those people taking the exam will be allowed to attend. Copies of the schedule will be available from the CA panel office.

4d. (FOUO) AWARDING OF "TECHNICAL TRACK MASTER" TITLES

(FOUO) Included among the Z Group personnel who received their "Tech Track Master" titles on 29 January 1997 are:

[redacted]

(b)(3)-P.L. 86-36

Congratulations to all!!

//

5. (U) TECHNICAL ARTICLES

5a. (FOUO) "Z071 - The Barbershop"
by [redacted]

(FOUO) Late in the summer of 1985 [redacted] assembled a group of mathematicians to work on a special project in support of both the Operations and COMSEC directorates. [redacted]

[redacted]

significant preliminary work, but they were never assigned an organizational designator.) The team was housed in the only space available in the OPS3 building at the time: a storage closet that was to be refurbished as a barbershop. (Legend has it that the DDI at that time, Walter Dealy, was envious of the barbershop in OPS1.) Henceforth, the group was affectionately dubbed the "Barbershop". The name has persisted to this day.

(FOUO) In its eleven years of existence, the Barbershop has occupied six organizational designators [redacted]) and eight locations (including a trailer at OPS3, three sites on the second floor of OPS1, and our current home in the basement of OPS1). The move out of OPS3 came as the original Barbershop mission was (successfully) completed and [redacted] triumphantly lobbied for the group to remain together as an operations organization.

(b)(3)-P.L. 86-36

(FOUO) Adopted by P12 in 1989, incorporated into Z51 with the formation of Z group, and recently renamed [redacted] with the dissolution of Z5, the Barbershop continues to thrive as a small team of mathematicians called on to solve, or at least study, a wide range of exciting, difficult problems.

(FOUO) Today's Barbershop consists of [redacted] assigned individuals, [redacted] of whom are currently out of the office: leading research pods, serving as a team chief in Z2, on PCS to La Jolla, teaching, or on diversity tours. We are also hosting two fabulous integrees, one from the cryptomath program and one from the C development program. Current members have contributed to all eight Director's Summer Programs, the last seven of which as technical directors (to include the summer of 1997). Two of us have been chairpersons of the math hiring committee while another two are currently serving on the Z tech track review panel. In the past year we have completed duty as instructors for both MA246 and MA414. Thus, we reach out to the community in many important ways.

(TSC) What, then, is the role of the Barbershop today? To answer this it is worth a quick look back. In the past, we often found ourselves in the enviable position of having the time to think hard about problems that others, more directly responsible for the timely production of plaintext, did not. As a result of this luxury, the Barbershop developed

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted]

(FOUO) However, like most organizations, we see that cryptomathematics and cryptanalysis will have to fundamentally evolve, perhaps even reinvent itself, to meet the demands presented by a world where our ability to influence encryption both from an INFOSEC and SIGINT perspective is diminishing. Being able to adapt to requirements quickly, to stay current with the breathtaking pace of technology, and to bet correctly where the next breakthrough will come is going to be ever harder to accomplish without groups of talented individuals focused on these goals. The Barbershop sees itself as one of these groups and, as such, we recently took the initiative on a number of projects that pushed us across several disciplines and organizational boundaries.

[redacted]

(C SCO) Despite the fact that we have recently been involved in several high profile, speculative projects, what we do best is respond to the problems brought to us by the CA community. As a small organization attempting to respond to the individual needs of a much larger one we always run the risk of being accused of working on only those problems where we can expect a quick solution and not tackling the harder ones. From our perspective, we cannot work on all the problems sent our way -- there are just too many -- so we make conscious decisions to focus on those for which we think we can make progress. (Again, this is a luxury we realize that many in the CA community do not enjoy.) Nevertheless, certain projects like [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(FOUO) The Barbershop continues to work hard on being responsive to the CA community in ways that will encourage individuals to come to us with their questions and problems. We want to work with you, to deliver tools, techniques, and solutions that will make your job easier. The best success for us is when we cooperatively solve your problem employing new mathematical techniques that prove to be generally useful. The freedom we are given in selecting and working the problems you give us is a responsibility we take very seriously. Therefore, we encourage everyone to find out more about what we are doing and help us to find ways that will make us even more effective.

(FOUO) With luck and lots of hard work the Barbershop will continue to be a vital resource for the CA community as we all discover and define the evolving roles of cryptanalysis and cryptomathematics.

(C SCO) But don't forget about us when that interesting [redacted] problem comes along ....

"""

5b. (U) Matt on Math
By: [redacted]

(FOUO) "A Brief Introduction to Factoring, Part II"

INTEGER FACTORING, PART II

(U) Last month we discussed integer factoring using sieving techniques. The run time of a sieving algorithm is a function of the number we want to factor, i.e. they run a really long time if the number we want to factor is big. There are other algorithms, probabilistic in nature, with expected run times given as a function of the smallest prime factor!

(U) Suppose we want to factor the composite integer N. Further, suppose that the (yet unknown!) prime p is some prime factor of N. If p has the property that p - 1 is smooth (recall, smooth means that it's only divisible by small primes) then the "p - 1" alogrithm is a good choice for finding p.

(U) The p - 1 algorithm is based on some simple number theory.

(b)(3)-P.L. 86-36

[redacted]

Choose an integer b that is a multiple of all (or most) of the integers less than some bound B. We might select b = B! for instance. Now, choose a random integer a in the interval

[2, 3, ..., N-2]

and compute

a^b (mod N).

This is traditionally done by "successive squaring". For example, to compute a^8 we actually compute

a^8= ((a^2)^2)^2

reducing modulo N at each step. If the exponent is not itself a power of 2 then we use the base two (binary) expansion and go. For example, to compute a^291 we first expand 291 in binary

291 = 100100011 (binary)

which is nothing more than a sum of powers of 2

291 = 2^8 + 2^5 + 2^1 + 2^0 = 256 + 32 + 2 + 1

so we compute

a^291 = a^256 * a^32 * a^2 * a

by calling successive squaring three times and multiplying (mod N) the results together.

(U) Okay, recall that we have a fixed value for b and a random value for a. We computed a^b (mod N) by the successive squaring method just described. Now, we compute

d = gcd(a^b mod N, N)

using the Euclidian Algorithm. If d is NOT a non-trivial divisor of N, choose a new value for a and go at it again, otherwise d = p.

(U) The p - 1 algorithm has its best chances of working when b is divisible by all the positive integers less than a bound B, and further when p is a prime divisor of N so that p - 1 is smooth with respect to B.

(U) Example: Maple session showing the facorization of 1537 using p - 1. (Maple is a symbolic algebra system that runs on Agency computers.)

```
> N:=1537:
------------------------------------------------------------------------
> B:=isqrt(N);

                                  B := 39
------------------------------------------------------------------------
> B:=factorial(39);

          B := 20397882081197443358640281739902897356800000000
------------------------------------------------------------------------
> for a from 50 to 60 do igcd(Power(a,B) mod N,N) od;

                                    1
                                    1
                                    1
                                   53
                                    1
                                    1
                                    1
                                    1
                                   29
                                    1
                                    1
------------------------------------------------------------------------
```

Clearly, 1537 = 53 * 29.

5c. (U) Science and Engineering Society

~~(FOUO)~~

The Science and Engineering Society
presents

[redacted] (b)(3)-P.L. 86-36

speaking on

DATA COMPRESSION

[redacted]

Thursday March 13, 1997 10:00 a.m. R&E Symposium Center

(FOUO) Data compression is a technology which affects much of the signalling environment. This talk explores the current state of the art in compression methods and where future developments appear to be leading, as well as the impact on the mission of NSA.

(FOUO) [redacted] is a cryptanalyst and computer scientist who has worked in several different offices in DO, and has worked aspects of the NSA mission from the collection, processing, archival and cryptanalysis perspectives. She is currently an analyst in the [redacted]

(FOUO) Her paper on "Data Compression" won second prize in the 1996 Science and Engineering Society Technical Paper Contest.

(FOUO) For information on or membership in The Science and Engineering Society please contact Tom Kline [redacted] 961-1354 [redacted]

(b) (3)-P.L. 86-36

(FOUO) This presentation will be broadcast on Newsmagizine channel 17

OPEN TO ALL FULLY CLEARED PERSONNEL

//

6. (U) COMMUNITY SERVICE

6a. (FOUO) CA Support to FBI
by [redacted]

(U) I think that I have one of the best jobs here at the Agency. Not only do I get to teach Cryptanalysis classes at the National Cryptologic School to Agency personnel, but from time to time, I get to help on some other interesting projects involving Cryptanalysis.

(FOUO) [redacted] the FBI's cryptanalyst (perhaps you remember him from his CA-305 talks), spent several months in our office a few years ago taking some introductory level CA courses. As you may know, [redacted] gets to work on some pretty interesting things involving terrorists, stalkers, and prisoners to name a few. But when [redacted] gets stuck on a problem, he turns to his Cryptanalysis professors for guidance.

(U) Just last week, [redacted] called me about an enciphered message that he had received as part of an ongoing investigation. [redacted]

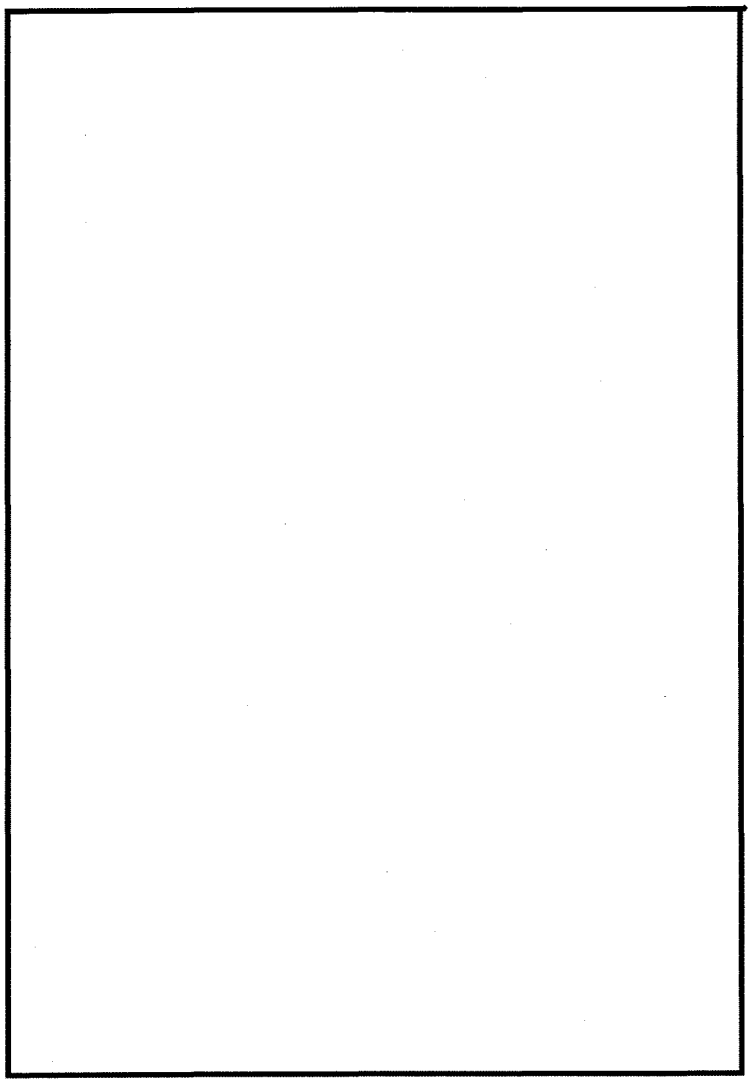
(b) (6)
(b) (7) (C)
(b) (7) (E)
OGA

FBI

[redacted]

(b) (3)-P.L. 86-36

[redacted]



(b) (6)
(b) (7) (C)
(b) (7) (E)
OGA

FBI

(U) Certainly a lot more exciting than "Reference your message number," isn't it?

****

6b. (U) Reprint from CRYPTOLOGIC ALMANAC

(U) A Brief Look at Public Cryptography
by Joseph Yankowski, Center for Cryptologic History

This article is UNCLASSIFIED in entirety.

The roots of cryptography run deep into the past. However, one has to look back only to World War II to trace the beginning of issues arising in public cryptography. The war caused the U.S. government to support many researchers in cryptology. One of those was Dr. Claude Shannon of Bell Laboratories, whose research led to the development of a new branch of mathematics known as information theory. His major work was published in 1948, and the following year he prepared a treatise on secrecy systems that applied information theory to cryptology.

Shannon's work was theoretical and dealt with the broad principles governing cryptography. He was not concerned with the finite elements which comprise the tools of the contemporary cryptologist. Consequently, most academic efforts in unclassified cryptography were of theoretical interest and had little practical value.

The 1950s brought the beginnings of the technological revolution that transformed the computer from an exclusive tool for science into a tool for business. By the mid-1960s, security weaknesses in remote time-shared computer systems were becoming apparent. Some of the weaknesses could be overcome by cryptography, which led to an ever-increasing industrial investment in cryptographic research. The academic community would not be far behind.

A prime example of industrial cryptologic research was the work performed at International Business Machines (IBM). In the late sixties the company decided to embark on studies involving cryptology as part of an overall program in data security initiated by IBM

(b)(3)-P.L. 86-36

president Thomas Watson, Jr. He believed that data communications was an up-and-coming thing and that, historically, encryption had been the only way to ensure the security of data transmissions. Watson's decision resulted in IBM's establishing a cryptologic research group at its laboratory in Yorktown Heights, New York. The group, led by Horst Feistel, developed a cryptographic algorithm, which was given the code name Lucifer.

In 1971 IBM was asked to quote on a special product for Lloyd's Bank in England. The product was a cash dispensing terminal that included a device to prevent spoofing. IBM chose to meet the protection aspects of the requirement by developing a version of its Lucifer cryptoalgorithm for the terminal. With the development of the cipher, the research group concluded its work.

IBM then formed a group to develop data encryption products based on the Lucifer algorithm. To lead the team, the company chose from its ranks Walter Tuchman, holder of a Ph.D. in information theory from Syracuse University. He assembled a data security products group that included IBM employee Carl Meyer, an electrical engineer with a Ph.D. electromagnetic theory from the University of Pennsylvania. By the end of 1971, it had become clear to Tuchman and Meyer that the Lucifer algorithm would not be strong enough in its original form for general-purpose use. The Lucifer cipher was adequate for the Lloyd's cash issuing system where a coded system prevented customer passwords printed on ID cards from being read and misused. The system would not, however, withstand intensive cryptanalytic attacks over a period of time.

Consequently, Tuchman and Meyer spent the next two years (1972-74) working to strengthen the Lucifer. At the same time, they subjected their improvements to "validation." They used cryptanalytic experts to try to find flaws in the algorithm that would enable an attacker to crack it.

After completing their work, and convinced of a strong product, Tuchman and Meyer began to develop products based upon the algorithm. The products included the model 3845 data encryption device, a desktop unit intended to operate at the ends of a data communications link between a modem and a terminal or a modem and a computer. The model 3846 was a rack-mounted version of the 3845. The group also developed the Cryptographic Subsystem, a hardware and software data encryption system intended to be used on large multiterminal 370 systems to protect data transmissions and on-line files.

Our next article will discuss the involvement of the National Bureau of Standards in public cryptography.

---

7. (U) Problems and Puzzles
by [redacted] (b)(3)-P.L. 86-36

7a. (U) Answers to last month's puzzle: Pirate Treasure

This article is UNCLASSIFIED in entirety.

A pirate ship captures a treasure of 1000 golden coins. The treasure has to be split among the 5 pirates, named Pirate 1, Pirate 2, Pirate 3, Pirate 4, and Pirate 5. Each pirate has the following important characteristics:

*) Infinitely smart
*) Bloodthirsty
*) Greedy

Beginning with Pirate 5, they each make a proposal on how to split up the treasure. This proposal is either accepted or the pirate is thrown overboard. A proposal is accepted if and only if a majority of the pirates agrees on it. (All pirates vote on a proposal, including the one who makes it. A majority is more than half - thus, if there are two pirates and the vote is 1-1, someone gets thrown overboard. A pirate would rather get zero coins than get thrown overboard.)
What proposal should Pirate 5 make?

Solution:

The idea behind the solution for this puzzle is that a pirate will accept a proposal only if he knows that in case he would not accept the proposal, he would get less of the treasure.

The best method to solve this is to build up from 1 pirate, up to 5. If there was only one pirate, he would get all the treasure. If there were two pirates, Pirate 2 would have to give all the treasure to Pirate 1 just in order to stay alive. All other proposals would be rejected by Pirate 1. Now suppose there are three pirates. Pirate 3 needs the agreement of one of the other two. Greedy Pirate 2 would agree with any proposal in which he gets more than 0 coins. (Otherwise, neither pirate agrees with Pirate 3, so he gets tossed overboard, leaving 2 pirates, in which case we have already seen that Pirate 2 gets nothing.) So the best proposal for Pirate 3 is to keep 999 coins, and give 1 to Pirate 2, and 0 to Pirate 1. Now suppose there are 4 pirates. He needs the agreement of 2 of the other 3. It is easiest just to give 1 coin to Pirate 1, and 2 to Pirate 2, and keeping the other 997 for himself. If either Pirate 1 or Pirate 2 disagreed with this, we'd end up in the 3 pirate situation, and we have seen that Pirate 1 and Pirate 2 get less in that situation. But there are five pirates. Pirate 5 needs the agreement of two of the other three. The best way to do this would be to give Pirate 1 two coins, and Pirate 3 one coin, and keep the other 997 for himself. Same reasoning - if this was rejected by either Pirate 1 or Pirate 3, we'd end up in the four pirate situation, and we have seen that both pirates get less in that circumstance.

So the final solution to the question is: Pirate 5 should make the (b)(3)-P.L. 86-36

following proposal: Pirate 1 gets 2 coins, Pirate 2 gets 0 coins, Pirate 3 gets 1 coin, Pirate 4 gets 0 coins, and Pirate 5 gets 997 coins.

Slight variations on the above solution are possible. Congratulations go to the following solvers:

[redacted]

(b)(3)-P.L. 86-36

8b.(U) March Puzzle: The Prisoner's Balls

This solution is UNCLASSIFIED in entirety.

The following puzzle was taken, with permission, from the web pages of "The Grey Labyrinth," on the outside web. You can visit at: [redacted] Send all solutions to

In far off Puzzlania, a prisoner waits on death row. By custom, the night before a prisoner is to be executed, he plays a game, either of chance orskill, it is the judge's discretion. This game will decide whether the prisoner will indeed die, or have his sentence commuted.

This particular prisoner was presented with a game that was perhaps a little of both. Before him are two large urns. One urn contains fifty black balls, the other fifty white balls. Tomorrow, the executioner will, while blindfolded, draw a ball randomly from one of the two urns. If it's black, it's curtains for the prisoner. If it's white, his sentence will be commuted to life. The prisoner wants very much to live, and is pleased with the current state of affairs that his chances of living are fifty-fifty. He is then presented with an option - he may change the contents of the urns. He can swap white balls for black, move balls from urn to urn, etc. There is a stipulation that when he is done, there must be fifty white balls and fifty black balls between the two urns - he can't eat some of the black balls or paint them or anything. Further, he can't leave either urn empty.

It occurs to the prisoner he might be able to help his situation by moving the balls so that there were twenty-five of each color in each urn, then making sure the white balls were on top. But the executioner might have guessed this, and may shake up the urns. Worse yet, he might deliberately reach to the bottom of the urn he chooses.

Is there another way the prisoner can help himself?

9.(U) EDITORIAL CORNER

REMINDER: Submissions for the April issue are due by March 26th.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

(b)(3)-P.L. 86-36

[redacted]

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2, DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR" DATE OF SOURCE: 3 SEP 1991

[redacted]

9/24/2010

~~TOP SECRET//COMINT~~

(~~C~~) *POC:* [redacted] *info*
(U) *Last Modified: 10/30/2002 11:42:21*
(U)PE EXTERNAL PAGE

(b)(3)-P.L. 86-36

****
* TALES OF THE KRYPT *
****
April 1997

//
****

++
//

(~~FOUO~~) TABLE OF CONTENTS:

1. Perspective

2. Calendar of Events

3. KRYPTOS Society News

4. Word from the CACP

5. Technical Article

6. Community Service

7. Problems and Puzzles

8. Open Letter to Our Readers

9. Editorial Corner

//
1. (~~FOUO~~) PERSPECTIVES - Each month this newsletter features the perspective of a Senior on a topic of his/her choice. This month we are pleased to publish Part I of an article by [redacted] Chief Z4.

~~~~~~

"MAKE THAT SEPARATE BUSSES, PLEASE" (~~FOUO~~)

(b)(3)-P.L. 86-36

(~~FOUO~~) As at least one of my predecessors in this column has suggested, it's an honor to be asked to give my perspective in CA. Those of you who've been in any of the relevant CA courses, or who've graduated from CMP training, or who've toiled long and hard in any of a host of computer science classes in order to get professionalized will immediately recognize that we never met in those circumstances. Unlike most of you, I am not a professional in the cryptanalytic sciences, so my perspective is, indeed, different.

(~~S~~C) Not long ago I had dinner with [redacted] (now at Ottawa) who had been NSA's principal liaison officer at Cheltenham in the early 90s. [redacted]

(b)(1)
(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

9/24/2010
~~~~~~

[redacted]

(~~FOUO~~) I liked this story for a lot of reasons. Those of you've who've been assigned to England might acknowledge the traffic risk as substantial. But the real appeal of the story, for me, is its illustration of where our precious advantage over adversaries really resides - in the knowledge, intellect and skills of the people who do this work. Since coming into Z I have had numerous opportunities to see firsthand just how much our successes have depended upon individuals and their abilities to use their creativity and resourcefulness to solve problems.

"""""""

4b. (FOUO) CAPQE

(FOUO) The CA PQE will be held on May 6 & 7 this year. The format for the PQE is a two-day, four-hours-per-day written test with eight questions presented each day. PQE review sessions will be held during the month of April, and will be scheduled during lunch hours so as not to interfere inordinately with office work time. It is strongly suggested that aspirants prepare for these sessions by working the questions from the previous examinations. Since some of the review sessions will be held in small conference rooms, only those people taking the exam will be allowed to attend. Copies of the schedule will be available from the CA panel office.

5. (U) TECHNICAL ARTICLES (b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

5a. (FOUO) Highlights from the Fall '96 MiniSCAMP
By: [redacted], MiniSCAMP Chair

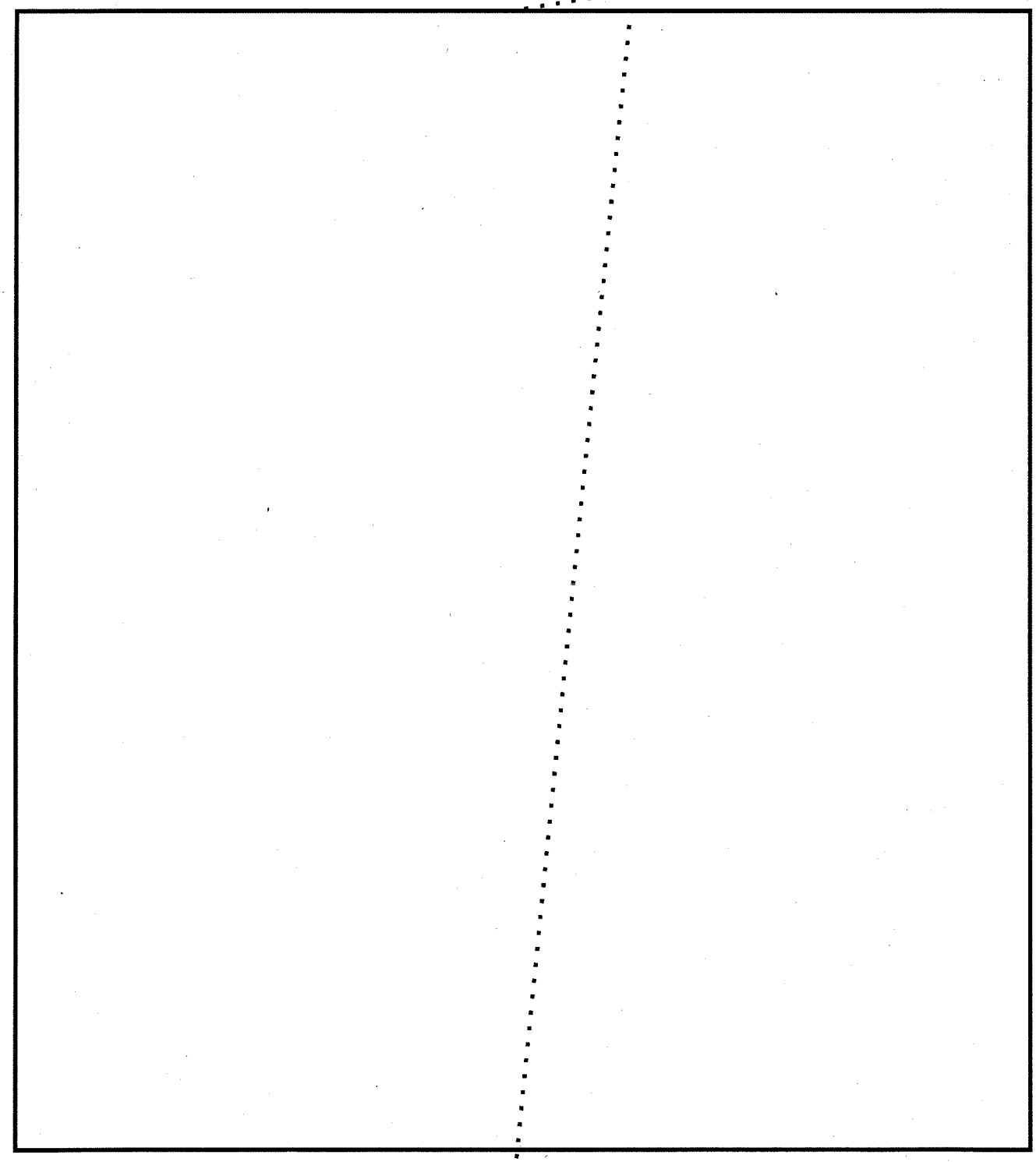
(C-CCO) The Fall '96 MiniSCAMP was held Oct. 15 - Nov. 22 at IDA-CCS. Thirty-four mathematicians, cryptanalysts, and engineers from Z, C, G, K, Q, R, IDA-CCS, and IDA-CCR-P worked on a variety of [redacted] Nineteen technical talks providing background information and explaining the MiniSCAMP problems were presented in the first five days.

[redacted]

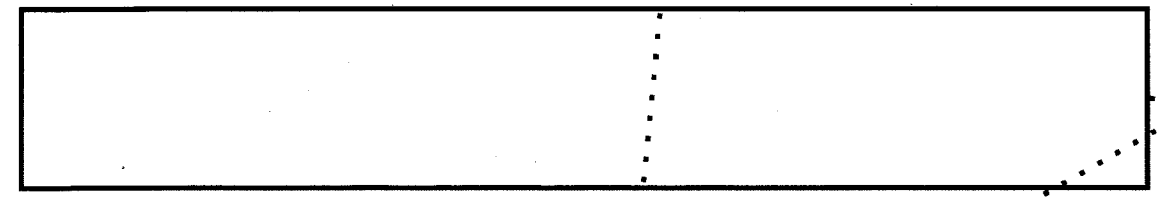
[redacted] (b)(3)-P.L. 86-36

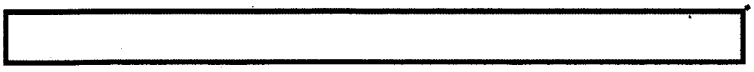
9/24/2010

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



(b)(3)-P.L. 86-36





[redacted]

(FOUO) A report containing more information about the technical accomplishments of the Fall 96 MiniSCAMP is being prepared and will be posted on the web at:

[redacted] (b)(3)-P.L. 86-36

The schedule of technical talks, which were videotaped, can also be found there. Contact the Z Technical Library, Headquarters Building Room 2A114, or [redacted] to make arrangements to borrow a tape.

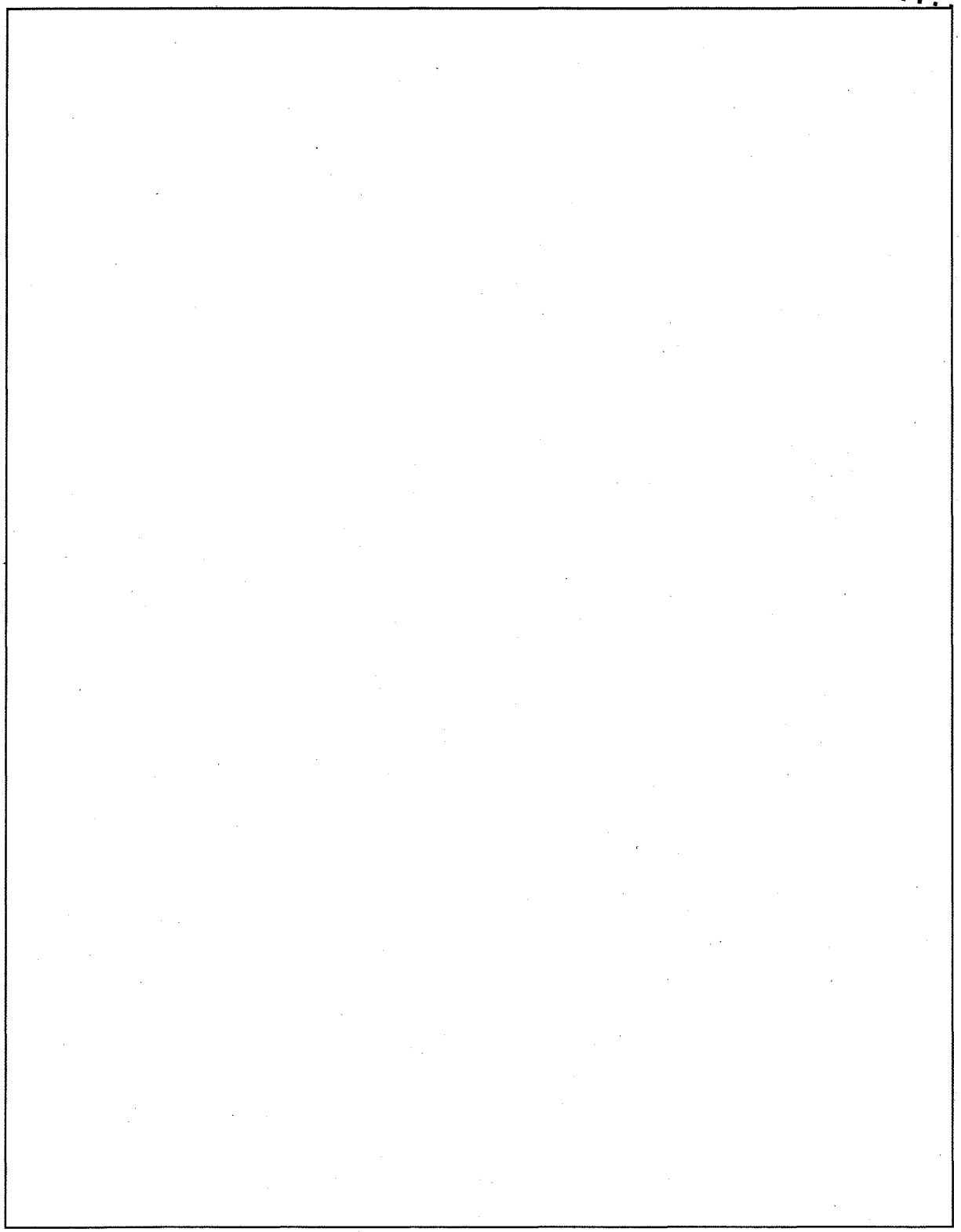
5b. (U) Matt on Math
By: [redacted]

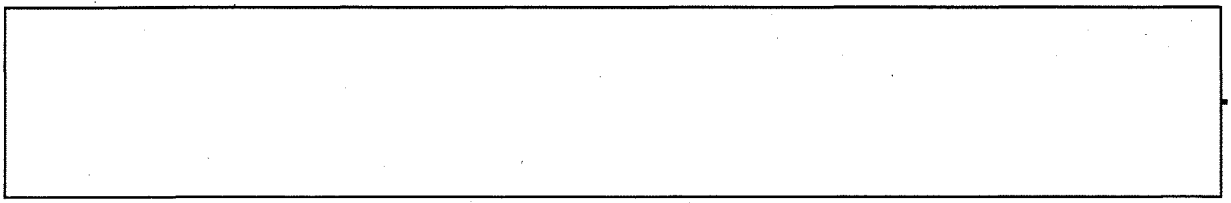
[redacted] (b)(1) (b)(3)-P.L. 86-36

[redacted]

[redacted] (b)(3)-P.L. 86-36

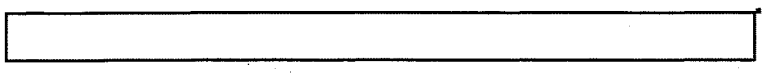
[redacted]





(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36



[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

5c. (U) New Largest Prime Number

This article is UNCLASSIFIED in its entirety and is a direct reprint.

NEW LARGEST PRIME NUMBER recently discovered by Cray has 378,632 digits (that would fill about 12 newspaper pages). Finding prime numbers helps researchers learn new techniques for speeding up mathematical operations. They are important in cryptography too. Primes do not occur in predictable sequences, and there's no formula for generating them other than to test millions of random numbers. Cray had discovered the previously largest prime number as well. By extrapolation, they predict a million digit prime in 2007. (Breakthrough #14 17Sep96)

5d. (U) Modem Supports Data Rates Up to 115.2 kbps at Three Kilometres

This article is UNCLASSIFIED in its entirety.

This report contains unclassified data which was obtained through commercial databases. If you would like further information on this article contact the Main library, located in room 1S042 (OPS1) on [redacted] the FANX library, located in room B7128 (FANX 3) on or the R&E library, room R1C075 on [redacted]

Computing Canada ..JJ: Computing Canada; March 3, 1997: p. 046.

TEL AVIV, Israel -- RAD Data Communications has introduced its SRM-6AV asynchronous high-speed modem designed to accommodate increased bandwidth requirements of traditional async applications in campus environments. The modem enables users to provide 115.2-kbps transmission throughout their campus facilities over two twisted pairs. A standalone unit measuring 4.3 by 2.1 by 0.9 inches, the SRM-6AV reaches a transmission range of three kilometres at 115.2 kbps and five kilometres at 19.2 kbps. RAD Data Communications; Phone: 972-3-6458181; Web Site: http://www.rad.com.

THIS IS THE FULL TEXT: COPYRIGHT 1997 Plesman Publications Ltd. (Canada)

6. (U) COMMUNITY SERVICE

(b)(3)-P.L. 86-36

6a. ~~(FOUO)~~ Mentoring by [redacted]

~~This article is classified FOUO in its entirety.~~

[redacted]

Recently I circulated an advertisement within NSA as follows: "At the Howard County Mathematics, Science and Technology Fair at River Hill High School on the 13th of March, there was a project on cryptography done by an eleventh grade student at Oakland Mills High School in Columbia, MD. This student created his own encryption technique and then tested it. The 'new' encryption algorithm generates random encoded messages so that even if the original messages are identical, the encoded messages will be different. While this encryption method is quite modest by our standards, the student demonstrated some ingenuity and promise. If properly guided, this (clearly highly motivated) student could have a bright future for himself, and perhaps a greedy thought, for us too."

"This student has been seeking a mentor and asked me if I could find him a mentor (at NSA). An NSA'er with some cryptologic background would probably be an ideal mentor for this student."

I have 'found' a mentor for this student. However, NSA is lending a helping hand to the local community in a number of ways, including tutoring students at Meade High School and MacArthur Middle School (as part of the Adopt-A-School program). This tutoring is done as part of the work day (e.g. administrative leave is granted for civilians). If you would be interested in helping students who request tutoring assistance in any of the subjects taught at the school, such as math, science, computer science, English, foreign languages, reading, writing, or social studies, then please get in touch with [redacted]. If you have no personal interest, then please forward this announcement to anyone whom you feel may be interested in tutoring these students.

"""""""

this, and may shake up the urns. Worse yet, he might deliberately reach to the bottom of the urn he chooses.

Is there another way the prisoner can help himself?

Solution:

The prisoner moves all the balls save for one white ball into one urn. There is a fifty-fifty chance the guard will select this urn and save his life. In the other urn, there is a 49.99 chance of being saved. This moves his net chance of survival up to a hair under 75%. Many methods of proof are possible, and this is easy to do by exhaustion.

(FOUO) Congratulations go to the following solvers: [redacted]

[redacted]

7b.(U) April Puzzle: (courtesy of [redacted]

This puzzle is UNCLASSIFIED in its entirety. (b)(3)-P.L. 86-36

This is an extension of an old chestnut.

The chestnut is this: You are walking along a road and come to a fork. You know that one road goes to Heaven and the other goes to the other place, but you don't know which is which.

By the fork stand 2 figures.
One figure always tells the truth, the other always lies, but you don't know which is which.
You are allowed to ask one question, and it must be at only one figure (your choice of question and figure) to discover the way to Heaven.

The question should have a YES/NO answer. (This is an attempt to try and keep the "truthful" and "deceitful" answers well-defined.)

The answer to the chestnut is to ask one figure
"If I asked the other figure, 'Does the left fork go to Heaven?',
what would the response be?"

Whoever you ask, you get told a lie.

(Comedians sometimes propose that you should ask the question "Does the left fork go to Heaven?" but aim it at the figure with the halo, rather than the one with the horns and tail.
We shall treat this suggestion with the contempt it deserves.)

The extension is that, when you get to a fork, there are 3 figures present. One always tells the truth and one always lies. The third is unpredictable. You can ask 2 (YES/NO) questions in order to find the way. What questions do you ask, to whom, to find the way to Heaven?

(FOUO) Send all answers (as well as other puzzle ideas) to [redacted]
([redacted]

(b)(3)-P.L. 86-36

[redacted]

"""""""

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

(b)(3)-P.L. 86-36

TOP SECRET//COMINT

(U) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:22
(U)PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
May 1997

//
****

++
//

(~~FOUO~~) TABLE OF CONTENTS:

1. Perspective: [redacted] "Leadership in the Cryptosciences"

2. Calendar of Events

3. Word from the CACP:

3a. March Certifications

3b. Thank You

4. Technical Article

4a. [redacted] Chief, R51: "Mathematicians Going Where They Have Never Gone Before: The Applied Mathematics Program"

4b. Matt on Math: "New New Largest Prime Number, or Mersenne Primes and Perfect Numbers"

4c. [redacted] "More on Prime Numbers"

4d. [redacted] "Life as an Integree"

5. Community Service

5a. Various Summer Math Programs

5b. [redacted] "The Director's Summer Program at the National Security Agency: Cryptologic Mathematics for Exceptional Undergraduate Mathematicians"

5c. [redacted] "Mathematics Networking Program: An Open Call for Members to Help New Mathematicians"

5d. CLA 32nd Annual Banquet

5e. CCWG Fifth Annual Conference on Computer Communications, Call for Abstracts

6. Problems and Puzzles: Reprint of April Puzzle

[redacted] (b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

7. Editorial Corner

(b)(3)-P.L. 86-36

//

1. (FOUO) PERSPECTIVES - Each month this newsletter features the perspective of a Senior on a topic of his/her choice. This month we are pleased to publish the thoughts of [redacted], Chief Z071.

(b)(1)
(b)(3)-P.L. 86-36

Leadership in the Cryptosciences (U)

(S) Over the last two years several experiences have led me to reconsider long held views about the roles and responsibilities of leadership in the cryptanalytic community. The uncertainty, evident at every level, of how to prepare for (and in many cases react to) a secure target environment that resists classical cryptanalysis has blurred the once clear distinctions of the roles and requirements of the different CA offices. Moreover, as our target set is clearly beginning to operate in a more heterogeneous crypto environment, we are seeing the need for a more interdisciplinary skill mix to [redacted] The experiences alluded to convince me of two things: in the near term, the seeds of leadership will have to be sown at the feet of the analyst, and the formal distinctions between cryptanalyst, cryptomathematician, and computer scientist must disappear. In the following I will describe some of the events that have shaped my perspective.

(C) Early in the fall of 1995 Tom Lessard (then Chief of Z, since retired) asked me to lead a group with the goal of producing a report outlining opportunities for Z in the "global intelligent network." I certainly did not understand what that meant at the time, but I did know that people were starting to fear a future in which classical cryptanalysis would not be successful in exploiting our targets. Then, as now, people spoke of freely available, secure encryption saturating communications over a cheap and reliable internet.

(FOUO) There was considerable discussion, early on, about the proper makeup of the group. Management wanted to be sure the right people were working on the right problems in the right spaces.... Well, you get the idea. Nevertheless, a group was assembled (primarily Z071, but also top notch people from Z2 and IDA-CCS). We immediately began to discuss among ourselves what direction the study should take. Over and over we asked: just what is the problem we are trying to solve? It was very difficult to break out of the traditional mind-set that expects problems to be clearly delineated and the avenues of attack finely drawn.

(S-CCO) Nevertheless, after twice-daily meetings in which we aggressively debated conflicting views of the future, the group seemed to converge, at least intellectually, on a picture that has proven, over the decidedly short term, to be very accurate. The resulting paper, easy to read and accessible to a wide audience, entitled "Z Group Opportunities in the Global Intelligent Network", is more relevant today than ever as attack strategies it recommends have actually been realized in operations.

(b)(3)-P.L. 86-3

(S-CCO) After the paper was completed, a Z off-site was convened to discuss means of implementing the report's recommendations. Management wanted to be sure the right people were working on the right problems in the right spaces.... Well, you get the idea. Fortunately, [redacted] took the burden onto themselves to form the [redacted] a recommendation of the report. This group of about a dozen individuals immediately began to search out new, non-traditional opportunities that might lead to target exploitation. I won't report on all the wonderful work this team has done for lack of space. However, it is worth noting that [redacted] and its leadership are directly responsible for the creation of the [redacted] an exciting, very recent initiative to cross organizational

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

[redacted]

all, the CA community can take pride not just in the significant strides it has made in exploiting opportunities it was not even considering a short two years ago, but also in the tremendous influence the analyst has had in setting the pace of this revolution.

~~(FOUO)~~ My point in telling this story is to presage what I believe is the way, at least for the near term, that cryptanalysis will evolve: teams of analysts committing themselves to discovering solutions to ill-defined problems - not waiting for direction from a senior management team that is justifiably apprehensive about where to direct dwindling resources.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(S//CCO)~~ Most people take as a given that we are in the midst of an explosive (and very exciting) information age that is being driven by breathtaking new digital technologies. [redacted]

[redacted] No one wants to bet wrong. Yet decisions must be made today that will affect our ability to thrive in the future. The input to these decisions must come from those actively working the problems. The current indecisiveness and lack of specificity from senior leadership (some of NCS-21 comes to mind) derives less from the character of those leading us than >from the lack of a spirit of entrepreneurship by those working the problems closest to the technologies we must defeat. In short, we must shape the future for ourselves.

(U) I would like to conclude with a brief analogy. My alma mater, the University of Rochester, recently shook the academic community by announcing the effective closing of its mathematics department. The graduate program was to be eliminated and the staff reduced by at least one half. Adjunct faculty would be hired to teach the bulk of the undergraduate curriculum. The problem was two-fold. Firstly, the other scientific departments (astronomy, physics, engineering) found that the math department was not adequately training its students. Indeed, they were finding it necessary to teach their own, more finely tailored, math courses. Secondly, the math department at Rochester, small to begin with, did not receive a high national ranking in a U.S. News and World Report survey. The university felt this would make it difficult to attract the best graduate students and the most lucrative grants. In a word, the department was expendable. Fortunately, the worldwide academic community was able to successfully lobby the university to reverse its decision (but at the cost of a substantially reduced graduate program and smaller department overall).

(U) The problems Rochester experienced are by no means isolated. In many universities the following pattern has been repeated. Mathematics departments, deeming computer science not sufficiently "pure", jettisoned it. Applied and computational mathematics, driven in large part by computers, was treated similarly. The consequent rise of computer science and applied mathematics

(b)(3)-P.L. 86-36

[redacted]

programs and departments in this country has come largely at the expense of departments of pure mathematics.

(S) We must be very careful not to treat cryptomathematics and cryptanalysis as "department" enclaves. In every sense we should be embracing new disciplines, cryptanalytic in nature, but not necessarily "pure". Otherwise we are destined to suffer a fate similar to Rochester. Perhaps we should move from the cryptanalytic development program and the cryptomathematician program to a cryptoscience program that embraces all of the disciplines - computer science, cryptomathematics, cryptanalysis, engineering - that will be needed in equal measure to decrypt cipher well into the future. Let's not complain the game is unfair. Let us all do our part to rewrite the rules.

---

2. (U) CALENDAR

This calendar is FOR OFFICIAL USE ONLY in its entirety.

May 22	CLA 32nd Annual Banquet (see 5d. below)

PLAN AHEAD

Oct 6-10	CONSCRYPT '97 at GCHQ
Oct 20-24	CCWG 5th Annual Conference (see 5e. below)
Oct 29-31	Seventh Symposium on Cryptologic History

---

3. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

3a. (FOUO) NEWLY CERTIFIED CRYPTANALYSTS:

(FOUO) The Cryptanalysis Career Panel is pleased to announce the certification of the following cryptanalysts during March: (b)(3)-P.L. 86-36

[redacted]

3b. (U) The Cryptanalysis Career Panel wishes to thank everyone (organizers, speakers, etc.) who helped make last month's CA Conference a success.

---

4. (U) TECHNICAL ARTICLES

4a. (FOUO) Mathematicians Going Where They Have Never Gone Before: The Applied Mathematics Program
by [redacted] Chief, R51 (b)(3)-P.L. 86-36

(TSC) The availability of a number of extra hiring allocations late in FY96 created a unique opportunity for the NSA mathematics community. At the suggestion of Richard C. Proto, Chief R, a new development program for mathematicians was established in the Mathematics Research Division, R51. The Applied Mathematics Program (AMP) assembled its first class in September 1996

[redacted]

(b)(3)-P.L. 86-36

with [ ] new mathematicians. The goal of the program is to place some of the very exceptional new math talent that we have been able to attract into a diverse set of offices throughout the Technology Directorate, in much the same way that the Cryptologic Mathematics Program has served the Operations Directorate for over three decades. [ ] is the Technical Director of the AMP, and [ ] is the Program Administrator. They placed [ ] of the participants in K Group for their initial tours, and [ ] in offices throughout R Group. Most are focused on problems associated with global network intelligence, ranging from research on [ ] to the development of new techniques to process and extract information from massive data sets. They have formed synergistic relationships with computer scientists, engineers, and linguists, and the spirit of One Team, One Mission is strong within the group. Management throughout T has been extremely supportive of the program and a very impressive record of technical accomplishments has already been posted by the group. Participants of the program will take several diversity tours over a three-year period and then settle into a more permanent assignment.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(TSC) As is customary in development programs, members of the AMP began their work at NSA with some basic courses. Lectures on cryptologic mathematics, [ ] important technical problems in their assigned organizations. The applications of mathematics to cryptology are well known and have been developed over many years. But the full potential for applying mathematics to problems in emerging technology has not yet been realized. We are confident that the Applied Mathematics Program will bring the full power of mathematics to bear on these exciting problems.

4b. (U) Matt on Math
By: [ ]

(U) New New Largest Prime Number, or Mersenne Primes and Perfect Numbers

(FOUO) The April edition of _Tales of the KRYPT_ announced the September 1996 discovery of Slowinski and Gage that 2^1257787-1 is a prime with 378,632 decimal digits. In November 1996, Armengaud, Woltman et al. found the 35th known Mersenne prime as part of GIMPS -- The Great Internet Mersenne Prime Search. This number, 2^1398269-1, is a prime with 420,921 decimal digits.

(U) These primes come from a family of prime numbers known as Mersenne Primes, named after a French monk who lived in the early 1600s. He stated that 2^n - 1 is prime for n = 2,3,4,7,13,17,19,31,67,127, and 257, and is composite for all other values n < 257. Mersenne was wrong. We now see that

2^61 - 1 = 2305843009213693951 is prime,

(b)(3)-P.L. 86-36

2^89 - 1 = 618970019642690137449562111 is prime,

2^107 - 1 = 162259276829213363391578010288127 is prime,

and 2^67 - 1, 2^257 - 1 are composite. It wasn't until 250 years after Mersenne's death that any mistakes were found in his work.

(U) The following proposition is fundamental to the search for Mersenne primes.

[ ]

Proposition: If n is composite, then so is 2^n - 1.

Suppose that n is composite, then n = a * b with a > 1 and b > 1. From this we will explicitly factor 2^n - 1. First, recall from high school algebra that

$$x^b - 1 = (x - 1)(x^{b-1} + x^{b-2} + \ldots + x + 1).$$

This formula is valid for any positive integer b. You can prove the identity above simply by multiplying out the right hand side:

$$(x^b + x^{b-1} + \ldots + x^2 + x) - (x^{b-1} + x^{b-2} + \ldots + x + 1)$$

and noticing that all the intermediate terms cancel out, leaving us with x^b - 1. We now use this identity with x = 2^a, obtaining

$$2^n - 1 = 2^{a*b} - 1 = (2^a)^b - 1$$
$$= (2^a - 1)((2^a)^{b-1} + \ldots + 2^a + 1).$$

Since a>1, the first factor 2^a - 1 is nontrivial.

(U) The proper divisors of a number are the divisors that are less than the number itself. For example, the proper divisors of 6 are 1, 2, and 3. A number is called PERFECT if it is equal to the sum of its proper divisors. Hence, 6 is perfect because 6 = 1 + 2 + 3 and 12 is not. Can you find the next perfect number? There is a hint below.

(U) Perfect numbers and Mersenne primes are related. In fact, if 2^n - 1 is prime then 2^{n-1}(2^n - 1) is perfect. Take n=2 for example:
2^2 - 1 = 3 which is prime and 2(2^2-1) = 2*3 = 6 which is perfect. How does one prove this statement?

(U) Suppose 2^n - 1 is a prime. We'll just call it p. Then a complete list of the proper divisors of 2^{n-1} * p is given by

$$1, 2, 2^2, \ldots, 2^{n-1}, p, 2p, (2^2)p, \ldots, (2^{n-2})p.$$

We didn't list (2^{n-1})p since it is not a proper divisor. Now, the sum of the proper divisors is

$$1 + 2 + 2^2 + \ldots + 2^{n-1} + p(1 + 2 + \ldots 2^{n-2}). \quad [EQ\#1]$$

Using the algebraic identity from above with x = 2 and b - 1 = k we get the formula

$$1 + 2 + 2^2 + \ldots + 2^{k-1} + 2^k = 2^{k+1} - 1.$$

Applying this twice to [EQ#1] above gives us that the sum of the proper divisors of (2^{n-1})p is 2^n - 1 + p(2^{n-1} - 1). Now we write p as 2^n - 1 again:

$$(2^n - 1)+(2^n-1)(2^{n-1}-1) = (2^n - 1)+2^{n-1}(2^n - 1) - (2^n - 1)$$

$$= 2^{n-1}(2^n - 1).$$

Hence, 2^{n-1}(2^n - 1) is perfect.

(U) Euler showed that the only even perfect numbers are the ones of this form. It is widely believed that there are no odd perfect numbers. This, however, has not be proven.

(FOUO) There are 35 known Mersenne primes, hence 35 known perfect numbers. A

complete list of Mersenne primes can be found on WEBWORLD at

[redacted] (b)(3)-P.L. 86-36

(U) Hint: June 28 is a perfect day in a perfect month.

4c. (U) More on Prime Numbers

~~(FOUO)~~ [redacted] wrote to the KRYPTOS Newsletter Board as follows: "Someone might already have pointed this out but here goes anyway.

(U) The text below appeared in the April '97 Tales of the KRYPT announcing a "New Largest Prime Number" having 378,632 digits. The discovery of this prime was in 1996 (as the article says) but since that time (also in 1996) a new larger prime was found which has 420,921 digits. This larger prime number is 2^1398269 - 1.

(U) [Item in April _Tales of the KRYPT_.]
NEW LARGEST PRIME NUMBER recently discovered by Cray has 378,632 digits (that would fill about 12 newspaper pages). Finding prime numbers helps researchers learn new techniques for speeding up mathematical operations. They are important in cryptography too. Primes do not occur in predictable sequences, and there's no formula for generating them other than to test millions of random numbers. Cray had discovered the previously largest prime number as well. By extrapolation, they predict a million digit prime in 2007. (Breakthrough #14 17Sep96)"

~~(FOUO)~~ [redacted] suggested we contact [redacted] for further information. [redacted] advised us of the following URL in the NSA WEB (also cited in the "Matt on Math" column in this issue in 5b. above): "See [redacted] in particular, if you click on the latest prime exponent (1398269) you will get information on its discovery."

4d. ~~(FOUO)~~ Life as an Integree (b)(3)-P.L. 86-36
by [redacted]

[redacted]

~~(FOUO)~~ I was enrolled in the CMP class of 96 and found it to be a great experience. While I was confused by the huge organization that is NSA, at least I was with a group in the same position. I also had companions to share the trial of completing CA101, MA148 and MA246 in the first six months while also trying to get some work done in my first tour.

~~(FOUO)~~ Like my fellow CMPers, I took 6 month tours in various offices. [redacted] did not impose any requirement on where I should go other than that I should aim to get a range of experiences. In fact I found that one of the biggest advantages of being an integree was more independence. My main contact back home, that is with the people who decide my promotions, was sending monthly notes. Of course,

with independence comes responsibility. It was up to me to ensure that I was getting the appropriate experience and training.

(C-CCO) My experiences on tours were similar to those of my fellow CMPers. However, I was lucky to not have to deal with time cards! Despite the NSA's large size I was pleased to find good camaradarie in the teams where I toured. One interesting experience was working as part of an NSA team competing with my colleagues from [redacted] in a race to solve a cryptologic. When [redacted] won the race I felt mixed emotions. There was the disappointment of not being in the "winning" team and the satisfaction that the [redacted] had been first.

[redacted]

(b)(3)-P.L. 86-36

(FOUO) Being a foreigner does have its benefits as well. I found that people were more likely to have heard of me and remember me since I was the [redacted] integree" in the NSA math community. [redacted] or not, people have always been very open to me at NSA. I know that one of the greatest benefits I will bring back to [redacted] when I return will be my contacts here.

(FOUO) The plethora of seminars, talks, courses, and conferences overwhelmed me. With so many more events at NSA than at [redacted] I very much wanted to exploit the opportunities while I was here. But if I attended everything I found interesting I would barely have time to do my regular work!

(FOUO) My experiences as an integree were so positive that when I had a chance to extend my posting a year I grabbed it! But we all move on at some point and this September I will return to [redacted] after an extremely rewarding four years. For all I have learned and all the friends I made I am grateful. Any readers considering applying for an integration should go for it.

"""""""

The Director's Summer Program is the National Security Agency's premier outreach effort to the very best undergraduate mathematics majors in the country. Each summer we invite [redacted] exceptional students to participate in a 12-week program where they work directly with NSA mathematicians on mission-critical problems. The program is highly competitive and is intended primarily for students between their junior and senior year, but exceptional freshman and sophomores will also be considered. Graduating seniors will be considered too, but they must be enrolled in a mathematics graduate program for the fall.

The goals of the Director's Summer Program are to:

* Introduce the future leaders of the U.S. mathematics community to the Agency's mission and share with them the excitement of working on mathematics problems of national importance,

* Provide a deep understanding of the vital role that mathematics plays in enabling the Agency to tackle a diverse set of technical challenges,

* Encourage bright undergraduate mathematics majors to continue their study of mathematics and pursue careers in the mathematical sciences, and, of course, to

* Provide solutions to current operational problems.

(b) (3)-P.L. 86-36

The students participating in the program work on a broad range of problems involving applications of Abstract Algebra, Geometry, Number Theory, Combinatorics, Graph Theory, Probability, Statistics, and Analysis. During the first two weeks of the summer lectures on cryptologic mathematics. After the lectures, the students are presented with about 10 current problems and must choose which problems they will focus on for the summer. The outstanding work accomplished by each student is documented in the DSP year-end report. Students develop mathematical theory, apply what they learn to obtain real-time solutions, and experience the excitement of success built on hard work and innovation. Many students find the work at NSA very exciting and challenging and decide to return for several summers.

State of the art computing resources are available to all students. Programming is done in C in a UNIX environment. MATHEMATICA is available, as is the computational algebra package MAGMA and a variety of statistics packages.

Information about the Director's Summer Program is sent to over 300 colleges and universities across the United States each year. In addition, students who have scored well in the annual William Lowell Putnam Mathematical Competition are invited to apply. Because of the lengthy processing required, the deadline for applications is 15 October each year. To apply, students simply complete an application or send a resume. At least two letters of recommendation from faculty members familiar with their work, and a copy of transcripts through the current academic year is also required. All students must be U.S. citizens. Information should be sent to: Department of Defense, National Security Agency, Attn: S232 (DSP), Fort George G. Meade, MD 20755-6000. For additional information about the DSP, call [redacted] Program Administrator at [redacted] or send e-mail to [redacted]

5c. (U) Mathematics Networking Program: An Open Call for Members to Help New Mathematicians

This letter is ~~FOR OFFICIAL USE ONLY~~ in its entirety.

(b) (3)-P.L. 86-36

[redacted]

Hello,

We are coordinating this year's Mathematics Networking Program which is designed to help new mathematicians acclimate to the NSA mathematics community. Each new hire is paired with a current member of the mathematics community. The purpose of this is to give the new hire an initial contact into the internal network. The exact nature of this relationship depends on the parties involved.

We are asking that you, as a member of the mathematics network, join the program as a contact for a new hire. If you choose to help us, we will try to match you with an appropriate person. We anticipate hires into the CMP, AMP, and CDP, as well as directly into certain offices. Please feel free to let us know if you have any specific preferences which would affect how you are paired up.

We look forward to hearing from you.

[redacted] (b)(3)-P.L. 86-36

5d. (U) CLA 32nd Annual Banquet

This article is UNCLASSIFIED in its entirety.

The Crypto-Linguistic Association is pleased to announce the CLA 32nd Annual Banquet on Thursday, 22 May 1997, 1130 - 1330 at Fort George G. Meade Officers Club.

The Crypto-Linguistic Association is very fortunate to have for its guest speaker this year [redacted] language testing expert, teacher, author. (b)(6)

The topic of his talk is "A Debt Unpaid" -- a brief overview of the new foreign language standards for schools and a recounting of the influence of government language programs on the "outside world."

In addition, the winners of the 1996 Jaffe, Rochefort, and [redacted] Awards will be announced at the banquet.

Tickets went on sale 1 May 1997. (b)(3)-P.L. 86-36

5e. (U) CCWG Fifth Annual Conference on Computer Communications
Call for Abstracts

(~~FOUO~~) The Agency Computer Communications Working Group will hold its Fifth Annual Conference on Computer Communication from October 20-24, 1997.

(~~TSC~~) THEME: C2C and the SIGINT Process

Focus Areas:

"From RF to Consumer" -- consisting of case studies showing various aspects of the foreign intelligence target from signal access to the consumer of the information.

"Filling the Gaps" -- highlighting works in progress.

[redacted] (b)(3)-P.L. 86-36

"Future Directions" -- to include emerging technologies, Agency architecture plans, and other anticipated items.

"Miscellaneous" -- a catch-all to include updates from various working groups, training opportunities, and anything else.

~~(S-CCO)~~ Authors are invited to submit a short general paragraph to the CCWG Conference Committee describing a 15-, 30- or 45-minute talk, visual presentation or demonstration. It should be aimed at a general NSA audience. Themes for discussion may include, but are not limited to the following general problem topical areas:

- Successful analysis and targetting strategies.

[redacted]

- Inter-Agency collaboration.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) Schedule Deadlines

(U) One paragraph describing the talk due to the committee - 30 Jun 1997.
Notification of acceptance to author by CCWG - 1 Sept 1997.

~~(FOUO)~~ POC: Send Abstracts via e-mail to [redacted] (b)(3)-P.L. 86-36

//

6. (U) Problems and Puzzles

(U) Due to the shortness of time between publication of this month's _Tales of the KRYPT_ and last month's, the April puzzle is extended through May. We are reprinting it as a courtesy to those readers who do not have the April issue at hand.

(U) April Puzzle: (courtesy of [redacted]): (b)(3)-P.L. 86-36

This puzzle is UNCLASSIFIED in its entirety.

This is an extension of an old chestnut.

The chestnut is this: You are walking along a road and come to a fork. You know that one road goes to Heaven and the other goes to the other place, but you don't know which is which.

By the fork stand 2 figures. One figure always tells the truth, the other always lies, but you don't know which is which. You are allowed to ask one question, and it must be to only one figure (your choice of question and figure) to discover the way to Heaven.

The question should have a YES/NO answer. (This is an attempt to try and keep the "truthful" and "deceitful" answers well-defined.)

[redacted] (b)(3)-P.L. 86-36

The answer to the chestnut is to ask one figure "If I asked the other figure, 'Does the left fork go to Heaven?', what would the response be?"

Whomever you ask, you are told a lie.

(Comedians sometimes propose that you should ask the question "Does the left fork go to Heaven?" but aim it at the figure with the halo, rather than the one with the horns and tail. We shall treat this suggestion with the contempt it deserves.)

The extension is that, when you get to a fork, there are 3 figures present. One always tells the truth and one always lies. The third is unpredictable. You can ask 2 (YES/NO) questions in order to find the way. What questions do you ask, to whom, to find the way to Heaven?

~~(FOUO)~~ Send all answers (as well as other puzzle ideas) to [redacted]

7. (U) EDITORIAL CORNER (b)(3)-P.L. 86-36

REMINDER: Submissions for the June issue are due by May 23rd.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted] (b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

[redacted]

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

(b)(3)-P.L. 86-36

TOP SECRET//COMINT

(C) POC: [redacted] info
(U) *Last Modified: 10/30/2002 11:42:22*
(U) PE EXTERNAL PAGE

(b)(3)-P.L. 86-36

```
**********************************
*        TALES OF THE KRYPT      *
**********************************
```

June 1997

//
****

++
//

(U//FOUO) TABLE OF CONTENTS:

1. Calendar of Events

2. Word from the CACP:

   2a.(U) May Certifications, Intern Promotions, and Intern Awards

   2b.(U) 1997 PQE Statistics

3. KRYPTOS Society

   3a.(U) Annual KRYPTOS Literature Contest

   3b.(U) New Technical Talk Contest

4. Technical Article

   4a.(U) Matt on Math: "A Glimpse of the Shimura-Taniyama Conjecture"

   4b.(U) CRYPTOLOGIC ALMANAC: "Open Code"

5. Community Service

   5a.(U//FOUO) Briefing on US Encryption Export Control Policy

   5b.(U//FOUO) 6th Annual Cryptanalysis, Computing and Communications Conference

   5c.(U//FOUO) CLA Presents "Exotic Languages Month"

6. Problems and Puzzles

   6a.(U) Answer to April Puzzle

   6b.(U) June Puzzle

7. Editorial Corner

""
//

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

1. (U) CALENDAR

This calendar is FOR OFFICIAL USE ONLY in its entirety.

Jun 2-12 CLA Presents "Exotic Languages Month" (see 5c below)

PLAN AHEAD

Oct 6-10 CONSCRYPT '97 at GCHQ

Oct 20-22 6th Annual Cryptanalysis, Computing and Communications Conference (see 5b below)

Oct 20-24 CCWG 5th Annual Conference

Oct 29-31 Seventh Symposium on Cryptologic History

//

2. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

2a. (U) NEWLY CERTIFIED CRYPTANALYSTS:

(U//~~FOUO~~) The Cryptanalysis Career Panel is pleased to announce the certification of the following cryptanalysts during May:

[redacted]

(b)(3)-P.L. 86-36

Intern Promotions: [redacted] to GG-12

Intern Awards: [redacted] - SPCA

2b. (U) 1997 PQE Statistics

(U//~~FOUO~~) The annual CA PQE was given on May 6 & 7. [redacted]

[redacted]

//

3. (U) KRYPTOS SOCIETY NEWS

3a. (U//~~FOUO~~) KRYPTOS Society: Call for Literature Contest Papers

(U//~~FOUO~~) The annual KRYPTOS Society Cryptanalytic Literature Competition is now underway. The competition is open to all personnel at NSA, to personnel on field assignments, and to retirees (consistent with security considerations).

(U//~~FOUO~~) The papers may treat any topic in the broad category of professional cryptanalytic literature, including:

[redacted]

(b)(3)-P.L. 86-36

_____attacks and techniques relating to cryptanalytic problems;
_____cryptanalytic research;
_____history of cryptanalysis;
_____other subjects relating directly to cryptanalysis, e.g. target studies, cryptologic trends from the point of view of cryptanalysis, or computer support of a cryptanalytic problem.

(U//~~FOUO~~) The judges will consider the following criteria:

_____Is the paper an original discussion of a cryptanalytic subject?
_____Is the paper well written? Is the subject presented well? Can a reader with a suitable technical background but unfamiliar with the subject understand the paper and, by reading it, gain knowledge about the subject?
_____Does the paper constitute an important addition to the body of cryptanalytic literature?

(U//~~FOUO~~) Submissions may be written specifically for the competition. Papers written between July 1, 1996 and June 30, 1997 are eligible. Entries may carry a classification of up to TSC. Compartmented papers will be considered only in extraordinary cases.

(U//~~FOUO~~) Cash prizes totalling $250 will be awarded to first, second, and third place winners at the discretion of the judges. Additionally, papers may be awarded honorable mention at the discretion of the judges.

(U//~~FOUO~~) Anyone can enter a paper with the permission of the author. Neither the author nor submitter (if different) has to be a member of the KRYPTOS Society.

(U//~~FOUO~~) If you have any questions regarding this contest, please contact [redacted]

(U//~~FOUO~~) To enter, please submit four copies of your paper to [redacted] by July 31, 1997. Each copy should be submitted with two cover sheets: the name(s) and organization(s) of the author(s) amd title on one sheet, and only the title on the other to facilitate impartial judging. The competition results will be announced at the KRYPTOS Society Fall Luncheon in October 1997.

(b)(3)-P.L. 86-36

3b.(U) New Technical Talk Contest

(U//~~FOUO~~) The KRYPTOS Society announces its First Annual TECHNICAL TALK contest for the best technical presentation on a subject relating to cryptanalysis or one of its related disciplines. The contest will consider talks given during the period of 1 July 1997 thru 30 June 1998 with the winner(s) to be announced at the Fall 1998 KRYPTOS Luncheon in October. All talks must be videotaped and last at least 30 minutes. All KRYPTOS and CMI talks will be automatically entered in the contest. The winner will be chosen by a panel of four judges (three >from NSA and one from GCHQ).

(U//~~FOUO~~) Any questions regarding this contest should be addressed to the KRYPTOS Society president, [redacted]

(b)(3)-P.L. 86-36

[redacted]

4. (U) TECHNICAL ARTICLES

4a. (U) Matt on Math
By: [redacted] (b)(3)-P.L. 86-36

(U) A Glimpse of the Shimura-Taniyama Conjecture

(U) We all know that Andrew Wiles and Richard Taylor recently proved Fermat's Last Theorem using their proof of the Shimura-Taniyama conjecture for semistable elliptic curves.

(U) To give the reader a feel for the Shimura-Taniyama conjecture, let C1 be the elliptic curve given by

$$C1: y^2 = x^3 - 4x^2 + 16,$$

and let M_p be the number of points on C1 over GF(p). Over GF(5), for example, the point (0,1) is on C1 because

$$1^2 = 0^3 - 4*0^2 + 16 \pmod 5.$$

(U) By exhausting all possibilities, we see that the only other points on C1 defined over GF(5) are {(0,4),(4,1),(4,-1)}. Therefore, M_5 = 4. It is not difficult to see that the following table is true:

p	3	5	7	11	13
M_p	4	4	9	10	9.

Table 1

Let F1(q) be the the formal power series given by

```
q*product((1-q^k)^2*(1-q^(11*k))^2,k=1..infinity);
```

in Maple notation. Next define N_n to be the coefficient of q^n in F1(q),

```
sum(N_n*q^n,n=1..infinity);
```

(U) Expanding the product by hand or using Maple for n<= 13 (see postscipt), yields the following table of values:

p	3	5	7	11	13
N_p	-1	1	-2	1	4.

Table 2

(U) Finally, observe that M_p + N_p = p for p = 3, 5, 7, 11, and 13. The Shimura-Taniyama conjecture for the curve C1 implies

$$M_p + N_p = p,$$

for all odd primes p. This was first demonstrated for the curve C1 by

[redacted] (b)(3)-P.L. 86-36

Eichler and Shimura.

(U) We close by noting that the Shimura-Taniyama conjecture, which remains open, implies that for every rational elliptic curve C there corresponds a similar function F such that the coefficients of F completely determine the number of points on C for all odd primes [n.b., the conjecture requires that F(exp(2*pi*i*z)) be a modular form of weight 2 for a suitable congruence subgroup].

(U) Postscript:

Here is a short C program that generates Table 1.

```
#include

void main(void)
{
  register int i,j,k,C;
  int M_p[5] = {0,0,0,0,0};
  int p[5]   = {3,5,7,11,13};

  for(i=0;i<5;i++) /* for each field GF(p) */
    for(j=0;j simplify(expand(q*product((1-q^k)^2*(1-q^(11*k))^2,k=1..13)));
 q-2*q^2-q^3+2*q^4+q^5+2*q^6-2*q^7-2*q^9-2*q^10-2*q^12+4*q^13+q^11
```

just pull off the coefficients of q^3, q^5, etc.

4b.(U) Reprint from CRYPTOLOGIC ALMANAC: Open Codes

This article is UNCLASSIFIED in its entirety.

The question of "open codes" is an interesting one; they provide minimal security in most cases. But, caught without a cryptosystem, individuals still seek to protect their messages. We recently read of two interesting varieties of open codes.

The first was composed by the commander-in-chief himself, President Abraham Lincoln:

"Hq. Armies of the U.S., City Point, Va. 8:30 a.m., April 3, 1865

TINKER, War Department: A. Lincoln its in fume a in hymn to start I army treating there possible if of cut too forward pushing is He so all Richmond aunt confide is Andy evacuated Petersburg reports Grant morning this Washington Secretary of War BECKWITH"

The "decryption process," of course, is to ignore the ostensible address and signature, then read the telegram backwards, concentrating on the sounds rather than the actual words. This format resembled a transposition cipher actually in use by the Union Army; normally, important words were given substitutes from a code book, then the word order was scrambled.

The second example of an open code was detected by the Office of Censorship just after the United States declared war on Germany in 1917:

"PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE.

GRAVE SITUATION AFFECTING INTERNATIONAL LAW.

STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS.

YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY."

The code in this case was the initial letter of each word:

P.....E.....R.....S.....H.....I.....N.....G S.....A.....I.....L.....S

F.....R.....O.....M N.....Y J.....U.....N.....E I.

Whatever the merits of the open code in this instance, Pershing actually sailed from New York on 28 May.

SOURCES: David Kahn, _The Codebreakers_; Center for Cryptologic History, _The Friedman Legacy: A Tribute to William and Elizebeth Friedman_

[David A. Hatch, Center for Cryptologic History, [redacted]

//

5. (U) COMMUNITY SERVICE

5a. (U//~~FOUO~~) US Encryption Export Control Policy

(b)(3)-P.L. 86-36

(U//~~FOUO~~) The Z Women's Council presents [redacted] Z03, discussing her tour of duty at the Department of State facilitating issues relating to the US encryption export control policy.

** Calendar Appointment **

Date: 06/10/97
Start: 02:00 PM
Stop: 03:00 PM
What: Export Control Briefing
OPS 2B, 2B4118-6

POC: [redacted]

5b. (U//~~FOUO~~) 6th Annual Cryptanalysis, Computing and Communications Conference: Call For Papers

~~This article is classified FOR OFFICIAL USE ONLY in its entirety.~~

****
****
** **
** Call For Papers **
** **
** **
** 6th Annual Cryptanalysis, Computing and **

[redacted] (b)(3)-P.L. 86-36

```
**            Communications Conference                **
**                                                     **
**                 October 20-22, 1997                 **
**        IDA Center for Computing Sciences            **
**                 Bowie, Maryland                     **
**                                                     **
*********************************************************
*********************************************************
```

The C^3 ("C-cubed") Conference has traditionally been a forum for presenting recent work on computational issues related to cryptanalysis. Starting this year, as reflected by a name change, the C^3 Conference subject matter will be expanded to cover additional areas of computation and communication which relate to the mission of NSA.

Participation is encouraged in the form of either technical papers and extended abstracts or perspective/survey style talks in the following areas:

Traditional cryptanalytic computing issues: comparative performance studies, mapping techniques for parallel and distributed computing, algorithms and data structures for cryptanalysis, SPDs.

Platforms for cryptanalysis: Performance evaluations, programming and optimization strategies, networked workstations as computing platforms, porting issues, workstation versus supercomputer issues, Unix versus Windows NT.

Processing of digital data: computer to computer networks, data mining, high speed protocol processing and data compression.

Tools: languages and compilers, software and hardware reverse engineering, computer security analysis tools and techniques, programming environments.

Global systems: issues and results from the Unified Cryptologic Architecture, services-based architectures.

A session(s) will also be set aside for recent results of SCAMPs, PODs and other relevant workshops.

Authors should submit a one to two page abstract by June 20, 1997 via e-mail to [redacted]
with backup Cc: to [redacted]

The classification level should *not* exceed TOP SECRET CODEWORD and *should* be accessible by second parties. The abstract must be in "electronic form" and may be unformatted text, Tex, FrameMaker, Postscript, or other WEB compatible format. Material appropriate for a 30-minute presentation is requested. Please ensure that your abstract provides a description of your work sufficient for the Program Committee to adequately

[redacted] (b)(3)-P.L. 86-36

[redacted]

evaluate it.

Authors will be notified by August 1, 1997 and will be asked to submit an extended abstract by October 1 for inclusion in the conference proceedings.

If you have software or hardware systems you would like to demonstrate, either in conjunction with a talk or as part of a possible demonstration session, please include a brief statement describing the demonstration together with your platform/environment requirements.

Registration and other information for attendees will be forthcoming. Visit our WEB page at

[redacted]

Additional Questions may be directed to: (b)(3)-P.L. 86-36

[redacted] C^3 Conference Chair

[redacted]

5c. (U//~~FOUO~~) The Cryptolinguistic Association presents "EXOTIC LANGUAGES MONTH", 2 - 12 June

This article is classified ~~FOR OFFICIAL USE ONLY~~ in its entirety.

As part of its 1997 foreign language film series, the CLA Film Committee will present an unusual program of movies in "exotic" languages. All have English subtitles.

All films will be shown in the Ops 2B Conference Center Room 2B4118-1. Dates and times as below.

EVERYONE IS WELCOME!

Bengali: "Pather Panchali" (1955, 113 min.)

Daily hardships for an Indian family are seen through the eyes of a young boy named Apu, who dreams of leaving his remote Bengal village to visit the big city. Satyajit Ray's groundbreaking film. Music by Ravi Shankar.

2 June (Monday), 1100-1300
4 June (Wednesday), 1100-1300

Lapp: "Pathfinder" (1988, 88 min.)

Action-packed epic based on an old Lapland saga about a boy who plots revenge against bandits who killed his family. Nominated for an Academy Award.

3 June (Tuesday), 1100-1230
5 June (Thursday), 1100-1230

(b)(3)-P.L. 86-36

[redacted]

Slovak: "The Coward" (1961, 113 min.)
A thriller set in a Slovak village during the last days of World War II. A cowardly teacher risks his life to save victims of Nazis.

9 June (Monday), 1100-1300
11 June (Wednesday), 1100-1300

Wolof: "Touki Bouki" (1973, 85 min.)

A Senegalese drama about the struggles of two young lovers from Dakar who dream of travelling to Paris to find a better life. A landmark film in New African Cinema.

10 June (Tuesday), 1100-1230
12 June (Thursday), 1100-1230

Notes: Films generally start on time. Bring your lunch if you wish. You do not need to be a CLA member to attend. For more information about the film series or the CLA Film Committee, contact [redacted]

The CLA is the Agency's professional organization for linguists. For membership information, contact [redacted] or [redacted].

6. (U) Problems and Puzzles

6a. (U) Last month's puzzle (extension of old chestnut), courtesy of [redacted]

(b)(3)-P.L. 86-36

This puzzle is UNCLASSIFIED in its entirety.

The chestnut is this: You are walking along a road and come to a fork. You know that one road goes to Heaven and the other goes to the other place, but you don't know which is which. By the fork stand 2 figures. One figure always tells the truth, the other always lies, but you don't know which is which. You are allowed to ask one question, and it must be at only one figure (your choice of question and figure) to discover the way to Heaven.

The question should have a YES/NO answer. (This is an attempt to try and keep the "truthful" and "deceitful" answers well-defined.)

The answer to the chestnut is to ask one figure
"If I asked the other figure, 'Does the left fork go to Heaven?', what would the response be?"

Whoever you ask, you get told a lie.

(Comedians sometimes propose that you should ask the question "Does the left fork go to Heaven?" but aim it at the figure with the halo, rather than the one with the horns and tail.
We shall treat this suggestion with the contempt it deserves.)

The extension is that, when you get to a fork, there are 3 figures present. One always tells the truth and one always lies. The third is unpredictable. You can ask 2 (YES/NO) questions in order to find the

way. What questions do you ask, to whom, to find the way to Heaven?

Answer:

The first question must determine a person who is not unpredictable. That person can then be asked the same question as in the original problem. Perhaps the easiest solution is the following (slight variations are possible):
Let a, b, and c contain among them the truthteller, the liar, and the waffler. For question 1, ask a, "If I were to ask you if b is the waffler, would you say yes?" Note that if a is the liar, the introductory clause would cause him to lie about his lie, and thereby tell you the truth. If a tells the truth, the introductory clause is irrelevant. If a is the waffler, his entire answer is irrelevant, because you are guaranteed to be asking the next question to someone who is not unpredictable.

If the answer is yes, ask C, "If I were to ask you if the left path goes to heaven, would you say yes?"

If the answer to the first question is no, then ask B the same question.

If the answer to the second question is yes, then take the left path. If the answer is no, take the right path. (Unless, of course, you really don't want to go to heaven.)

Solutions were received from [redacted]

6b. (U) June puzzle (courtesy of [redacted] (b)(3)-P.L. 86-36

Extension of the previous puzzle.

Giving up on the three figures, you double back and decide to look for a back entrance. Sure enough, you eventually come to another fork in the road, guarded by a single enigmatic figure. As you approach, you pass a stone tablet, which informs you of some useful facts about your imminent encounter.

1. One road goes to heaven, and the other to ...(you get the idea by now).
2. An angel and a demon take it in turns to guard the fork.
3. Neither the angel nor the demon can speak. Each can communicate only by nodding and shaking his head.
4. The angel always tells the truth, and the demon always lies.
5. Each will answer just one yes/no question. A nod means '@@' and a shake means '@@'.

One of the '@@' is 'yes' and the other is 'no', but unfortunately the tablet is too worn for you to determine which is which.

Which one question do you ask the guardian of the fork? You can assume the demon lies fairly - he won't contradict what you already know or can deduce.

Send all answers (as well as other puzzle submissions) to [redacted]
([redacted]
(b)(3)-P.L. 86-36

[redacted]

//

7.(U) EDITORIAL CORNER

REMINDER: Submissions for the July issue are due by June 23rd.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

(U//~~FOUO~~) EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

(b)(3)-P.L. 86-36

\\

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2, DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR" DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

(b)(3)-P.L. 86-36

[redacted]

[redacted]

(U) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:22
(U) PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
July 1997

//
****

++
//

(U//FOUO) TABLE OF CONTENTS:

This Table of Contents is FOR OFFICIAL USE ONLY in its entirety.

1.(U//FOUO) Perspective: [redacted] UKLO, "Reflections: H Division, Z Group, and the Changing Nature of Our Work"

2.(U) Calendar of Events

3.(U//FOUO) Word from the CACP: Titling of New Members of the Cryptanalysis Tech Track

4.(U) KRYPTOS Society:

4a. KRYPTOS Society Talk: [redacted]

4b. CMI/KRYPTOS Night at Baysox Game

4c. Call for Literature Contest Papers

4d. New Technical Talk Contest

5.(U) Technical Article

5a. (U) Matt on Math: "Numerical Evaluations of Some Popular Constants"

5b. [redacted]

6.(U//FOUO) Community Service

6a. (U//FOUO) Z Women's Council Talk & Networking Event: "Taking Chances, Building a Successful Career at NSA" by [redacted]

6b. (U) Science & Engineering Society Talk: "The Use of Imagery in Electromagnetic Wave Propagation Prediction" by [redacted] and [redacted]

6c. (U) Women in Mathematics Society Talk: "Latent Semantic Indexing" by [redacted] R51

6d. (U//FOUO) Z Women's Council Talk: "Taking the Fear Out of Change" by [redacted]

6e. (U//FOUO) Z Women's Council Talk: "Briefing on US Encryption Export Control Policy" b[redacted], Z03

6f. (U) Undergraduate Training Program

6g. (U) NSA's Fifth Invitational Mathematics Meeting

7. (U) Problems and Puzzles

7a. Answer to June Puzzle

7b. July Puzzle

8. (U) Editorial Corner

(b)(3)-P.L. 86-36

(b)(3) - 10 USC 424
OGA
NGA

(b)(3)-P.L. 86-36

//

1. (U//FOUO) PERSPECTIVES - Each month this newsletter features the perspective of a Senior on a topic of his/her choice. This month we are pleased to publish the thoughts of [redacted] UKLO-3.

[N.B.: British spelling and usage have been preserved throughout this perspective.]

Reflections: H Division, Z Group, and the Changing Nature of Our Work (U//FOUO)

(U//FOUO) Those of you who have been on an overseas tour will know how quickly 3 years can pass. My time as UKLO-3 is rapidly coming to an end and it is a good time to reflect on the relationship between H Division and Z Group and the changing nature of our work.

(U//FOUO) Change has been a constant companion during the last 3 years -- it is hard to recall a time when we have not been anticipating some new

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

change within Z or H or in NSA and GCHQ at large. My predecessor saw the major upheaval that brought about the creation of Z Group but, as is inevitable with any major change, it has taken some time for the new organisations to bed down and this has not been made easier by the pressure to refocus our effort to prepare for the 21st Century.

(C//SI) GCHQ has not been immune from change and at times it appears that every change at NSA is mirrored by one at GCHQ (or vice-a-versa). In

(C//SI) Not all of the changes have been organisational, there has been a great change in the problems that we face as our targets modernise their communications practices. Increasingly the production analyst has

(C//SI) Change has also affected the Liaison Officer's job. When I was an integree at NSA in the early 1980's all communication

(C//SI) Apart from easing the and other information, email has helped to strengthen the co-operation on cryptanalysis that has been the core of the H/Z relationship. The relationship has been built on the long history of exchanges of integrees and visitors and these continue today. The advent of email has added a new dimension to this by allowing the formation of multi-agency teams

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(C//SI) These examples point to one of the key requirements of the future. In order for us to achieve our potential as Sigint organisations we need to maintain our close co-operation in

(C//SI) What about life as a liaison officer? I was an integree in the early

(b)(3)-P.L. 86-36

1980's in what is now called the CMP. That gave me an opportunity to work in a number of different areas and make many friends throughout NSA. Coming back as a liaison officer has allowed me to renew those friendships and make many more. I have learnt a lot in 3 years - as much about what goes on outside of the crypt community as what is happening within it - but I would have to say that the work is not quite as much fun as being an integree.

~~(C/SCI)~~ I have enjoyed living and working in the US and would like to thank everybody who has been so helpful over the last 3 years - it has really made my job easier. Perhaps I can repay some of your kindness if you ever visit Cheltenham - there are some good opportunities coming up with CONSCRYPT, ACE and SCAMP all to be held there in the next year. Otherwise, I will see you when I come back for my next tour. (I can always dream!)

---

2. (U) CALENDAR

This calendar is [redacted] in its entirety.

(b)(3)-P.L. 86-36

Jul 8 Z Women's Council Talk & Networking Event: "Taking Chances: Building a Successful Career at NSA" by [redacted]
1300-1500 in Headquarters, room 9A135
(see 6a below)

Jul 10 Science & Engineering Society Talk: "The Use of Imagery in Electromagnetic Wave Propagation Prediction" by [redacted] and [redacted]
1000 in R&E Symposium Center
(see 6b below)

(b)(3) - 10 USC 424
OGA
NGA

Jul 10 KRYPTOS Society Talk: [redacted]
[redacted] IDA/CCS
1300 in Friedman Auditorium
(see 4a below)

Jul 11 Women in Mathematics Society Talk: "Latent Semantic Indexing" by [redacted] R51
1100 in Headquarters, room 2A198
(see 6c below)

Jul 15 Z Women's Council Talk: "Taking the Fear Out of Change" by [redacted]
1300-1500 in Headquarters, room 9A135
(see 6d below)

Jul 17 CMI/KRYPTOS Night at Baysox Game
(see 4b below)

(b)(3)-P.L. 86-36

Jul 21 Z Women's Council Talk: "US Encryption Export Control Policy by [redacted] 1330 in Headquarters, room 9A135
(see 6e below)

Jul 31 Deadline for entering KRYPTOS Society Literature Contest
(see 4c below)

Aug 3-6 NSA's Fifth Invitational Mathematics Meeting
(see 6g below)

PLAN AHEAD

Oct 6-10 CONSCRYPT '97 at GCHQ

Oct 20-22 6th Annual Cryptanalysis, Computing and Communications Conference

Oct 20-24 CCWG 5th Annual Conference

Oct 29-31 Seventh Symposium on Cryptologic History

Mar 23-27 CARD '98 at CSE

---

3. (U/~~FOUO~~) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

This article is ~~FOR OFFICIAL USE ONLY~~ in its entirety.

A ceremony was held on Monday morning, 2 June, to confer titles on the following new members of the Cryptanalysis Technical Track:

(Attending) (Not Attending)

MEMBERS:

[redacted]

(b)(3)-P.L. 86-36

SENIOR MEMBERS:

[redacted]

[redacted]

[redacted]

(b)(3)-P.L. 86-36

MASTERS:

[redacted] Chairman of the CA Career Panel, presided over the event [redacted] Chief Z, presented the certificates. Congratulations to all!

//

4. (U) KRYPTOS SOCIETY NEWS

4a.(U) The KRYPTOS Society presents a talk by [redacted] IDA/CCS, entitled [redacted] in the Friedman Auditorium at 1315 (seating begins at 1300).

Talk Abstract:

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U//FOUO) This talk will be videotaped. Please contact the Z Technical Librarian, [redacted] to obtain a copy of the videotape.

For Drag/Drop:

*** Calendar Date ***
Date: 7/10/97
Start: 1315
End: 1430
What: KRYPTOS Talk @ Friedman
Dealing with Less than Ideal Data Collection (U)

(b)(3)-P.L. 86-36

4b. (U) CMI/KRYPTOS Night at Baysox game

This article is UNCLASSIFIED in its entirety.

The KRYPTOS Society and the CMI are jointly sponsoring a family evening at the Bowie Baysox game on Thursday, July 17th. The Baysox play at the Prince Georges Stadium, Rt. 301, Bowie.

Game time is 7:05 with an optional all-you-can eat picnic beginning at 5:30.

Cost:
Picnic and reserved box seat: $20.00 each for adults
$15.20 each for children, ages 6-12
Picnic free for children under 6 years old
Reserved box seat only: $7.00, all ages
Parking: free

Picnic Menu (all you can eat):
Chicken, hamburgers, hot dogs, potato salad, baked beans, potato chips, watermelon, iced tea, lemonade. Beer and wine are available at extra cost.

To make reservations and purchase tickets for this event, please contact one of the following people:

Ops. 1: [redacted]
HQS:

OPS 2A:

FANX3:
R & E:
NBP:

All tickets must be purchased by noon on Friday 11 July.

Directions to the stadium:
From NSA, take Rt. 32 east to Rt. 3 south (which becomes Rt. 301 at the Rt. 50 interchange in Bowie.) The entrance to the stadium is on the left, less than 1/2 mile past the Rt. 50 interchange, at the second

[redacted]

traffic light.

4c. (U//~~FOUO~~) KRYPTOS Society: Call for Literature Contest Papers

This article is ~~FOR OFFICIAL USE ONLY~~ in its entirety.

The annual KRYPTOS Society Cryptanalytic Literature Competition is now underway. The competition is open to all personnel at NSA, to personnel on field assignments, and to retirees (consistent with security considerations).

The papers may treat any topic in the broad category of professional cryptanalytic literature, including:

_____attacks and techniques relating to cryptanalytic problems;
_____cryptanalytic research;
_____history of cryptanalysis;
_____other subjects relating directly to cryptanalysis, e.g. target studies, cryptologic trends from the point of view of cryptanalysis, or computer support of a cryptanalytic problem.

The judges will consider the following criteria:

_____Is the paper an original discussion of a cryptanalytic subject?
_____Is the paper well written? Is the subject presented well? Can a reader with a suitable technical background but unfamiliar with the subject understand the paper and, by reading it, gain knowledge about the subject?
_____Does the paper constitute an important addition to the body of cryptanalytic literature?

Submissions may be written specifically for the competition. Papers written between July 1, 1996 and June 30, 1997 are eligible. Entries may carry a classification of up to TSC. Compartmented papers will be considered only in extraordinary cases.

Cash prizes totalling $250 will be awarded to first, second, and third place winners at the discretion of the judges. Additionally, papers may be awarded honorable mention at the discretion of the judges.

Anyone can enter a paper with the permission of the author. Neither the author nor submitter (if different) has to be a member of the KRYPTOS Society.

If you have any questions regarding this contest, please contact [redacted]

To enter, please submit four copies of your paper to [redacted] by July 31, 1997. Each copy should be submitted with two cover sheets: the name(s) and organization(s) of the author(s) and title on one sheet, and only the title on the other to facilitate impartial judging. The competition results will be announced at the KRYPTOS Society Fall Luncheon in October 1997.

4d. (U) New Technical Talk Contest

This article is ~~FOR OFFICIAL USE ONLY~~ in its entirety.

The KRYPTOS Society announces its First Annual TECHNICAL TALK contest for the best technical presentation on a subject relating to cryptanalysis or one of its related disciplines. The contest will consider talks given during the period of 1 July 1997 thru 30 June 1998 with the winner(s) to be announced at the Fall 1998 KRYPTOS Luncheon in October. All talks must be videotaped and last at least 30 minutes. All KRYPTOS and CMI talks will be automatically entered in the contest. The winner will be chosen by a panel of four judges (three from NSA and one from GCHQ).

Any questions regarding this contest should be addressed to the KRYPTOS Society president, [redacted]

(b)(3)-P.L. 86-36

//

5. (U) TECHNICAL ARTICLES

5a.(U) Math on Math
By: [redacted]

(U) Numerical Evaluations of Some Popular Constants

This article is UNCLASSIFIED in its entirety.

This month we take a look at some examples from Richard Crandall's "Projects in Scientific Computation".

The computer package Maple instantly replied

2.71828182845904523536028747135266249775724709369995957496696762772407663035354759457138217852516642 7

when I typed evalf(E,100). This is the constant e -- the natural logarithm base -- evaluated to 100 decimals of precision. In fact,

[redacted] (b)(3)-P.L. 86-36

it didn't take Maple too long to spit out 100,000 decimal digits of e. How do Maple and Mathematica do it so quickly? This month we'll examine two methods for the numerical evaluation of e: "classical", and "continued fraction". We'll also see how to generate Pi with a continued fraction expansion.

Method 1: Classical. Recall from calculus that

$$e = \sum_{n=0}^{\infty} 1/n!$$

By default, Maple uses E = 2.718281828 [Note: "E" is the reserved symbol for "e" in Maple. We'll use both notations.] We can achieve this accuracy by summing the first 15 terms of the series above.

K	Sum(K)	error: E-Sum(K)
5	2.716666667	0.1615161e-2
10	2.718281801	0.27e-7
15	2.718281828	0.0

Comparing the 15th partial sum to the actual value of e (evaluated to 100 decimals), however, reveals differences beyond the 13th decimal place (Note 15! = 1307674368000).

Method 2: Continued Fractions. There is a beautiful continued fraction expansion of e:

$$e = 2 + \cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\ldots}}}}}}}}$$

An efficient way to evaluate a continued fraction expansion of the form

$$X = a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \ldots}}$$

is to set four initial values:

$$p_0 = a_0,\ p_{-1} = q_0 = 1,\ q_{-1} = 0$$

and iterate

$$p_n = a_n p_{n-1} + b_n p_{n-2}$$

$$q_n = a_n q_{n-2} + b_n q_{n-2}$$

for n = 1, 2, 3, etc. Then, x = Lim p_n / q_n as n -> infinity.

(U//FOUO) We can use this algorithm to carry out such a computation using Brouncker's formula for pi

$$4/\pi = 1 + \cfrac{1}{2 + \cfrac{9}{2 + \cfrac{25}{2 + \cfrac{49}{2 + \ldots}}}}$$

with a mathematica program. Increase len for greater accuracy. The following mathematica program yields

$$\pi \sim 3.14149265359004323845951838337481537878 7.$$

```
Mathematica 3.0 for Silicon Graphics
Copyright 1988-96 Wolfram Research, Inc.
 -- Terminal graphics initialized --

In[1]:= len=10000;

In[2]:= a=Table[2,{r,1,len}];
```

(b)(3)-P.L. 86-36

```
In[3]:= b=Table[If[r==0,0,(2r-1)^2],{r,0,len}];

In[4]:= pp=1; pc=a[[1]]; qp=0; qc=1;

In[5]:= Do[
        pf=a[[n]] pc + b[[n]] pp;
                qf=a[[n]] qc + b[[n]] qp;
                pp=pc; qp=qc; pc=pf; qc=qf,{n,2,Length[a]}]

In[6]:= Print[pf/qf," ",N[4/(pf/qf-1),40]]
```

5b. (U//FOUO) Cryptanalysis at Communications Security Establishment (CSE),
Eh! by [redacted] (b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) In conclusion, I agree with all the statements [redacted] made about the benefits of integration, but none more so than the one that anyone reading this who is considering applying for an integree position (particularly here at CSE) should go for it. The benefits obtained through the diversity of experience and perspective that you will be bringing back to the Agency are immeasurable. Plus you might end up having an annual hockey game named after you. Just ask [redacted]

---

6. (U) COMMUNITY SERVICE

6a.(U//~~FOUO~~) Z Women's Council Talk & Networking Event: "Taking Chances: Building a Successful Career at NSA"

This article is ~~FOR OFFICIAL USE ONLY~~ in its entirety.

(b)(3)-P.L. 86-36

Taking Chances: Building a Successful Career at NSA

[redacted]
Tuesday 8 July 1997
1300-1500 in 9A136

(b)(6)

[redacted] will discuss her experiences during her NSA career. As a former member of Z Group, she is familiar with Z issues and will focus her remarks on Z Group as well as broader Agency issues. This talk is open to all NSA employees.

[redacted] came to NSA in [redacted]

[redacted]

(b)(3)-P.L. 86-36

[redacted] will speak during the first hour. Immediately following there will be a networking reception (with food and refreshments) which all are welcome to attend. This will provide an opportunity for all individuals to meet [redacted] and mingle among themselves.

(b)(3) - 10 USC 424
OGA

NGA

POC: [redacted]

6b.(U) Science & Engineering Society: "The Use of Imagery in Electromagnetic Wave Propagation Prediction"

This article is UNCLASSIFIED in its entirety.

(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

The Science & Engineering Society presents [redacted] (Q64) and [redacted] (Q64) speaking on "The Use of Imagery in Electromagnetic Wave Propagation Prediction" on July 10, 1997 at 10:00 a.m. in the R&E Symposium Center.

[redacted]

(b)(3)-P.L. 86-36
(b)(6)

[redacted]

[redacted]

(b)(3)-P.L. 86-36

9/24/2010

(b)(3)-P.L. 86-36
(b)(6)

(b)(3) - 10 USC 424
(b)(3)-50 USC 3024 National Security Act of 1947 Section 102A(i)(1)
(b)(6)
CIA 3.5(c) Section 6 of the Central Intelligence Agency Act of 1949, 50 U.S.C. 3507
OGA

NGA
CIA

This is a classified presentation open only to Blue/Green/Gold badges.

The presentation will be broadcast over Newsmagazine Channel 17.

For information on or membership in the Science & Engineering Society contact Tom Kline [redacted] 961-1354 or [redacted]

6c. (U) Latent Semantic Indexing

(U//~~FOUO~~) The Women in Mathematics Society presents [redacted] R51, speaking on "Latent Semantic Indexing" on 11 July at ~~1100~~ in Headquarters, room 2A198. This is an application of the SVD to information retrieval.

(b)(3)-P.L. 86-36

6d. (U//~~FOUO~~) Taking the Fear Out of Change

(U//~~FOUO~~) The Z Women's Council presents [redacted], Chief [redacted] speaking on Tuesday, 15 July at 1300 in Headquarters, room 9A135.

[redacted]

(b)(3)-P.L. 86-36
(b)(6)

6e. (U//~~FOUO~~) US Encryption Export Control Policy

(U//~~FOUO~~) The Z Women's Council presents [redacted] discussing her tour of duty at the Department of State facilitating issues relating to the US encryption export control policy. Everyone is invited to attend.

** Calendar Appointment **

Date: 07/21/97
Start: 01:30 PM
Stop: 02:30 PM
What: Export Control Briefing
HDQS, 9A135

POC: [redacted]

6f. (U) Undergraduate Training Program

(U) How do you get the Agency to pay for your undergraduate degree? Ask the UTP students in your office this summer, or look for information in the July edition of the NSA Newsletter.

(b)(3)-P.L. 86-36

6g. (U) NSA's Fifth Invitational Mathematics Meeting

This article is UNCLASSIFIED in its entirety.

Please accept our invitation to the Fifth Invitational Mathematics Meeting for students of mathematics to be held on 3-6 August 1997. For this meeting we expect an audience of 130 undergraduate or graduate students of mathematics, many of whom participate in Undergraduate Research Experiences funded by NSA. The meeting will include unclassified technical presentations by both NSA mathematicians and our guests, panel discussions about technical careers at NSA, information on Agency-sponsored mathematics outreach efforts, and details on the hiring process at NSA. The conference will be opened by an address from the Deputy Director of the National Security Agency, Mr. William Crowell.

The goals of the conference are:
* to convey the technical depth and excitement of a mathematics career at NSA;
* to develop a network of contacts within and between students of mathematics;
* to make the point that NSA is sincerely interested in building the

[redacted]

math infrastructure of the mathematics communities, to discuss our current efforts in this area, and to learn how these efforts can be more effective;
* to explain the process of obtaining a job as a mathematician at NSA;
* to make it clear what we expect of a mathematician who is applying for a position at NSA;
* to describe the mathematics community at NSA and our internal training programs; and
* to LISTEN to our visitors so that we can better understand how to include these students in our future.

Attached is a tentative agenda for the meeting. We certainly hope you will be able to join us both Monday at the R&E and Tuesday at the Columbia Inn. If you choose to join us for any of the meals, you must make reservations and pay [redacted] by 25 July 1997.

Do not hesitate to contact [redacted] if you would like further information regarding the meeting.

We have high expectations for a successful Fifth Invitational Mathematics Meeting and we look forward to your participation.

Sincerely,

[redacted]
Chief
Mathematics Research Office

Fifth Invitational Mathematics Meeting
3-6 August 1997
Tentative Agenda

Sunday, 3 August Columbia Inn

1700 Registration
1800 Informal Dinner
1900 Majic Tricks, Card Shuffling, and Dynamic Computer Memories

Monday, 4 August R&E Building

0845 Welcome [redacted]
0900 Keynote Address Mr. William Crowell
0930 NSA Math Community Mr. Richard Proto
0945 Break
1000 Transversals in Row-latin Rectangles [redacted]
1030 On the Distribution of Fractional Parts
1100 Digital Representations of Speech
1130 Lunch (R&E Cafeteria)
1300 Panel - Careers at NSA
1400 What is Quantum Computing?
1430 Break
1500 Error-Correcting Codes
1600 Cryptologic Museum
1730 Dinner at Columbia Inn ($22.25)
1830 Engima- A German Puzzle, a Polish Solutio

Tuesday, 5 August Columbia Inn

0845 Administrative Remarks [redacted]
0900 Some Neglected Formulas in Linear Algebra [redacted]
0930 Student Presentations
1130 Lunch (Columbia Inn) ($18.45)
1230 Student Presentations
1630 Summary/Closing Remarks
1730 Bar-b-que at the Columbia Inn ($25.90)

Wednesday, 6 August

Trip to Washington DC

[redacted]

(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted]

[redacted]

Which one question do you ask the guardian of the fork? You can assume the demon lies fairly - he won't contradict what you already know or can deduce.

Answer:

In the same way as we used self-reference in the last problem to eliminate the lie, we use self-referece here to eliminate the effect of the uncertainty. Ask the guardian the following question: "If I were to ask you if the left road leads to Heaven, would you nod your head?" The chart below describes the possible outcomes:

Left fork goes to	Guard is a	A nod means	Then the answer is
Heaven	Angel	Yes	Nod
Heaven	Angel	No	Nod
Heaven	Devil	Yes	Nod
Heaven	Devil	No	Nod
Other Place	Angel	Yes	Shake
Other Place	Angel	No	Shake
Other Place	Devil	Yes	Shake
Other Place	Devil	No	Shake

If the guardian nods, go left; otherwise, go right (assuming, of course, that you want to go to heaven).

Solutions were received from [redacted]

7b.(U) July puzzle (courtesy of [redacted])

This puzzle is UNCLASSIFIED in its entirety.

Some months ago there was a puzzle about five pirates trying to divide up 1000 gold coins. This is an extension to that puzzle.

Once again we have five pirates, with the following six characteristics:

1) will do anything to avoid dying;
2) infinitely bloodthirsty;
3) infinitely greedy;
4) smart;
5) risk neutral: e.g. a half a chance of getting 10 coins is no better or worse than certainly getting 5; and
6) they are all ambivalent to each other.

They have a booty of 1000 gold coins to share, and reach the following agreement for doing it.

They will draw straws. The short one makes a proposal. Everyone votes. If a clear majority are in favor, the money is divided up. Otherwise, they throw him overboard (so he dies), and draw straws again.

What should the pirate who draws the short straw first propose?

Send all answers, as well as other puzzle submissions, to [redacted]

[redacted] (b)(3)-P.L. 86-36

8.(U) EDITORIAL CORNER

(U//FOUO) Special Congratulations to _Tales of the KRYPT_ Editorial Board member, [redacted], who won first place in the Agency's first "I AM AN AMERICAN" Festival Door Contest, in the category of "HQs. OPS2A, OPS2B". Her winning entry reflected "An American Collage."

REMINDER: Submissions for the August issue are due by July 23rd.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

(b)(3)-P.L. 86-36

(U//FOUO) EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

[redacted]

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

[redacted]

(b)(3)-P.L. 86-36

[redacted]

~~(S)~~ POC: [redacted] *info*

(U) *Last Modified: 10/30/2002 11:42:21*

(U) PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****

August 1997

//
****

++
//

(U) TABLE OF CONTENTS:

1. ~~(FOUO)~~ Perspective: Reprint of the Keynote Speech given by Mr. William P. Crowell, D/DIR, at the CA Conference

2. (U) Calendar of Events

3. (U) Word from the CACP

4. ~~(FOUO)~~ KRYPTOS Society: "The CSE Chapter of the KRYPTOS Society is Now Open for Business!" by [redacted]

5. (U) Technical Articles

   5a. ~~(S-CCO)~~ Matt on Math: [redacted] by [redacted], CMP Intern

   5b. (U) "Pete on PCS" by [redacted] GCHQ Integree

   5c. ~~(FOUO)~~ "Merits of Technical Diversification for Today's Problems" by [redacted]

   5d. ~~(FOUO)~~ "Update and Revision of the Cryptanalysis Classification Guide" by [redacted]

   5e. ~~(S-CCO)~~ [redacted] by [redacted] Z and [redacted] R51

6. (U) Community Service

   6a. (U) Z2 Summer Program Student Presentations

   6b. (U) Science & Engineering Society Talk: "Hybrid Technology Multi-threaded Architecture for High Performance Computing" by [redacted] R51 and [redacted] CCS

   6c. (U) Science & Engineering Society Talk: "Call for Papers"

7. ~~(FOUO)~~ Literary Notes: Review of Michael Drosnin's book, _The Bible Code_, by [redacted]

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

8. (FOUO) Problems and Puzzles by [redacted] (b)(3)-P.L. 86-36

8a. (FOUO) Answer to July Puzzle, courtesy of [redacted]

8b. (U) August Puzzle

9. Editorial Corner

****

//////////

1. (FOUO) PERSPECTIVES - Each month this newsletter features the perspective of a Senior on a topic of his/her choice. This month we are pleased to publish the text of the Keynote Speech delivered by Mr. William P. Crowell, D/DIR, on 23 April, 1997 at the CA Conference.

(FOUO) The information technology that we are seeing around us today is shaping our world and it is shaping the world of the cryptanalyst. It is shaping the world of those who are in the business of helping us to protect and exploit our communications targets.

(FOUO) The irony is that NSA helped to foster all of the technology challenges that are now really challenging us. We were really at the place where the technology of the computer was born. We were faced with an ENIGMA machine that we exploited using computing technology that we developed during WWII. (The ENIGMA, I am told, was a 2-to-the-64th bit keyspace machine; we only allow 2-to-the-40th encryption to be exported >from the United States at the present moment.)

(FOUO) And so we were the seedbed for today's computing technology. Whether it's the supercomputers that came from our intense interest in special purpose devices or whether it was the workstation that is so vital to the way we operate today, as an Agency we really were the place where it was all born, and we pushed computing far beyond what the market would have brought it to by this time without NSA. Then NSA and the Defense Department later on had enormous pulling effect on that technology.

(C) We also contributed mightily to all of the networking technologies that are available today. We participated in the original ARPANET. We adopted it as the backbone for our communications for the Agency more than 25 years ago, helped to develop it into the Internet and then saw it turned over to industry. In only six short years it has become the largest and fastest growing network that anyone could have possibly imagined, having grown at an exponential rate since its birth as a commercial entity.

(C) Now the market is driving the future of information technology - not us. We don't really control that industry anymore and we're not pulling it anymore. At best we're riding along with it into the Information Age. Our targets are getting more complex. The structures, the signals, and the networks are getting more complex, the volume is posing extraordinary problems for us and encryption, something that we held back as a commercial entity for a number of years, in fact, has been unleashed and will propagate and will be installed essentially worldwide. It isn't because we held it back that encryption didn't advance before. It's because it wasn't ready for advancement. Public key technology was not invented until the mid-70's and the network wasn't really invented for commercial use until the late '80's and early '90's. It was the

combination of the fact that the network is a huge party line but offers enormous opportunities for commerce and the fact that public key cryptography allowed, for the first time, a key management infrastructure that could be separated from a single trusted authority like NSA and could be operated in small enclaves for the purposes of commerce.

(S) Our tools are getting better as well, so we shouldn't look at all of this technology and say "Woe is me. It's really a terrible world. Look how bad things are getting." All of us are getting better tools, more powerful tools than ever before. And algorithms that we've developed in the last few years can actually be used today because of the enormous advances in computing and networking and you can run these algorithms either locally or in the network and achieve enormous results. We can also achieve enormous new capabilities as human beings because of the collaboration that the networks allow us to have and because of the computing capabilities that we can bring to collective endeavors through networks and groupware.

(S) So, while in some respects we did it to ourselves, we invented the technology that is making our problem harder, we also did it to ourselves in that we're inventing the new tools that are going to be better and make us more able to solve our future problems. The trick is going to be trying to manage those two in some kind of a sensible way.

(~~S CCO~~) Computer-based systems lend themselves to automated processing and can streamline the entire set of processes that we operate at the Agency. There are opportunities for not just [redacted] anymore, but for [redacted] and so on. And so we have powerful new opportunities using computers with networks to allow us to move to a software-based architecture and allow us to streamline everything that we do. So, if that's the case, what should we be doing differently for the future?

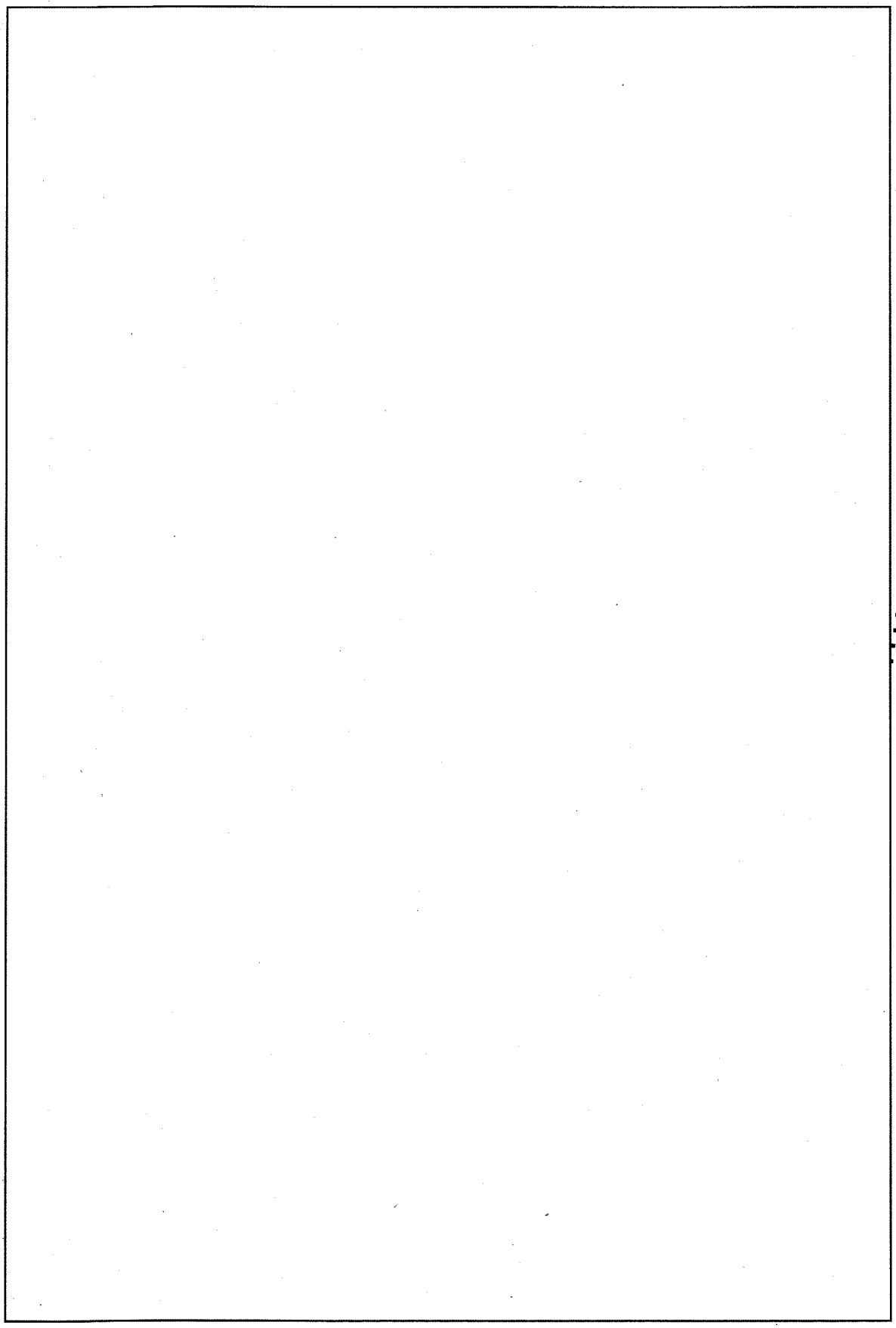
(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(~~S CCO~~) Now, I'm told that you're concentrating during this conference on [redacted] on signals analysis, and on [redacted] cryptanalysis. I intend to talk about those briefly but I'm going to add to that list three others: cooperation with industry, influencing standards, and breakthrough technologies, because I think those are also important to how we operate in the future.

[redacted]

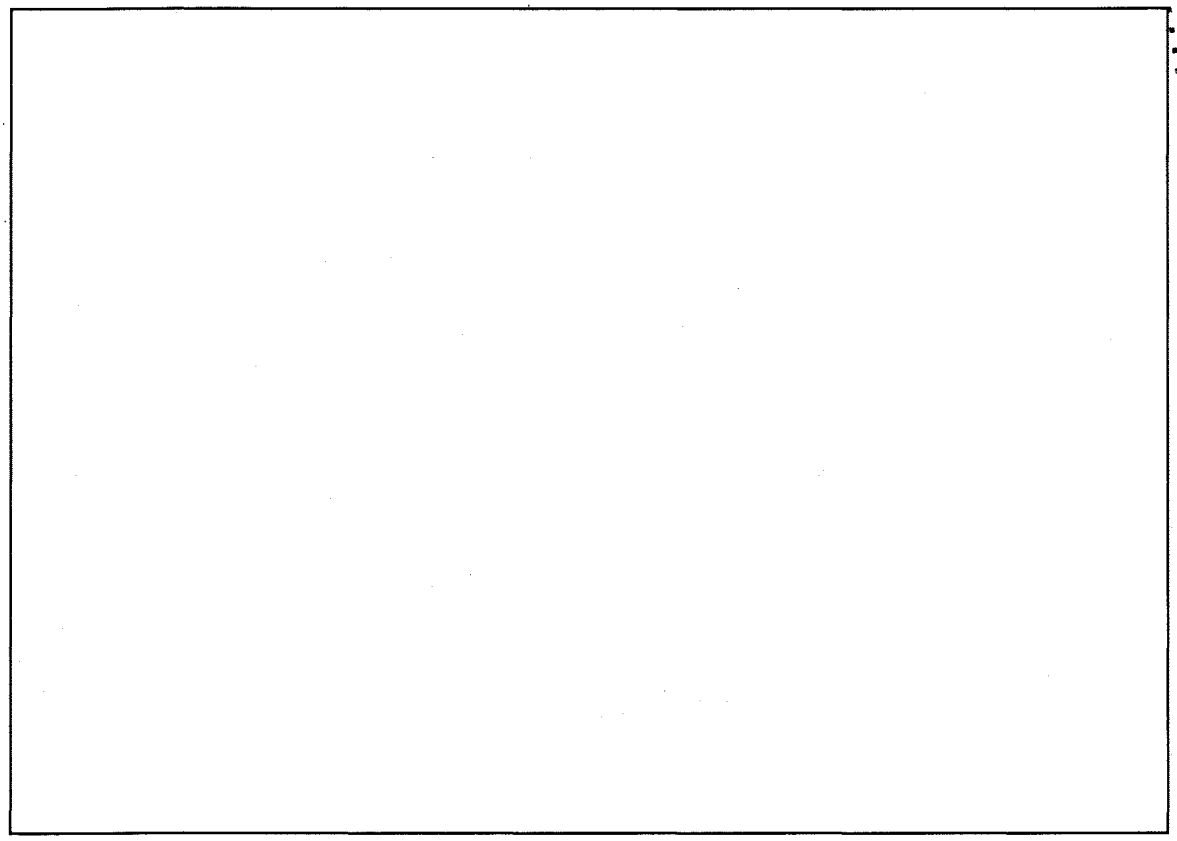
(b)(3)-P.L. 86-36

[redacted]



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

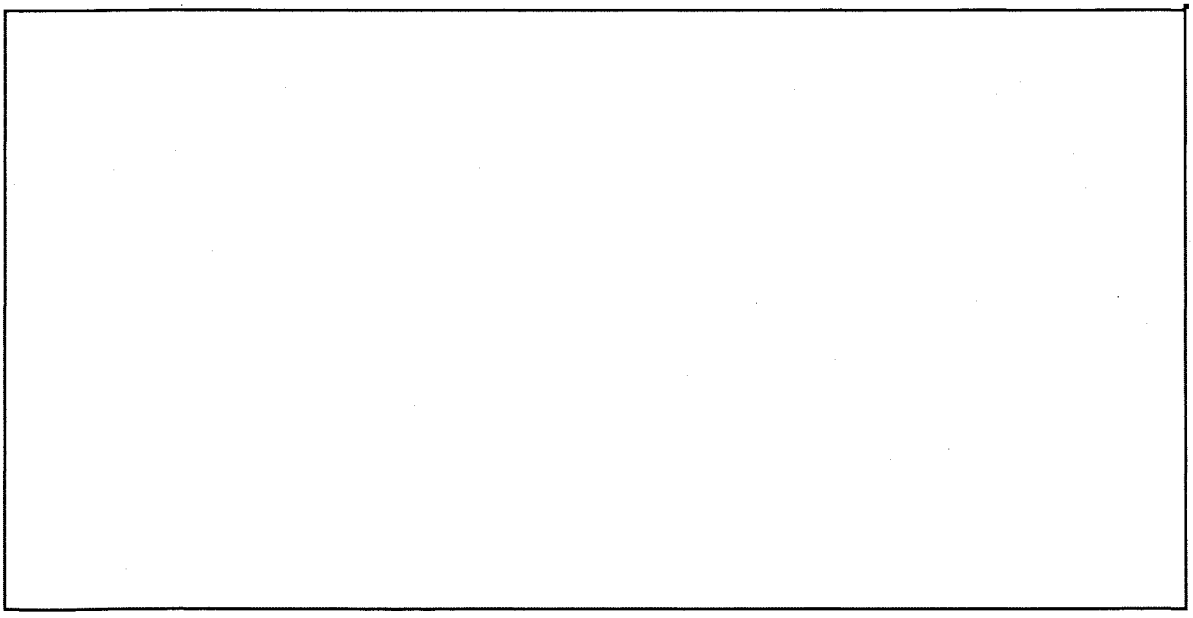
(b)(3)-P.L. 86-36

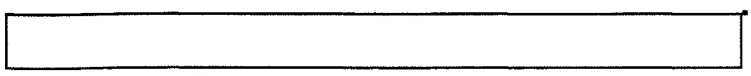


(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(C CCO)~~ In the Signals Analysis arena I would urge that we move as quickly as we can to a software-based capability. We cannot afford hardware-based solutions for signals analysis in the future. Signals will move too quickly and the cost is just too high. We need to be able to do signals analysis on the fly. We can't send everything to a central place and have it done by [redacted] We need to make sure that we put these software tools that can be used on the fly in the field so that they can be used by anyone and everyone to cut down on the number of unknown signals that really have to be worked by the experts and are really, in fact, unknown signals.

(b)(3)-P.L. 86-36





(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

~~(C)~~ A little bit about offense and defense synergy. Both information security and cryptanalysis concentrate on a common interest and that's vulnerabilities. The interaction between those communities is essential and they have to share their knowledge. The defense portion of this is important. The national interest is in being able to protect ourselves >from Information Warfare and from other forms of harm that can be brought to the nation. The nation is at risk and there is no sanctuary in the network. I believe (this is my vision for the network) that the network becomes to all of us much like what electricity has become to us in the past. Virtually everything we do, everything that we're interested in, will in some way be based upon the existence of the network. In my house when the electricity goes off, you can't do anything. You can't flush the toilets, you can't turn on the water, you can't do anything because it's all based on electricity. I talked this morning to the Head of Xerox Park down in Palo Alto California and they're working on a new technology that is the epitome of the influence of the network. They are working on MEMs (miniature electronic mechanical) devices to be used for future products in Xerox. Now what's Xerox's principal product? Copying. So imagine these thousands of little molecule-sized engines that can move paper around and then deposit things on it called printing. Well, that's the way people are thinking now about networks - in micro engines, in macro engines - but networks are carrying on a lot of the interaction and a lot of the work. So, we're going to have a lot of vulnerabilities in the future based upon how all of these networks connect. [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted] We also have to foster the interaction that is important to both the cryptanalytic field and the INFOSEC field. So I would like to urge you to foster interaction in the future, not only within the cryptanalytic community, but with signals analysts, engineers, computer scientists, and with those who are in the INFOSEC business as well.

~~(C)~~ Finally, let me just say something about the three principal areas of challenges that I see facing us. I've been talking primarily about technical challenges, and your fourth session is going to really address one of the most difficult of those; that is, if you think you know how to stay up and if you think you know how to protect what you know and leverage it to be able to do your job, getting the people and training

(b)(3)-P.L. 86-36

[redacted]

the people and developing the people to be able to keep up with those challenges is probably the biggest challenge of all. Now there are going to be legal challenges. Just the fact that Information Warfare is possible has already brought new interesting legal challenges to us in terms of our authorities to establish the Information Operations Technologies Center. There are always the legal challenges of how do we do our job and make sure it not only doesn't focus on U.S. persons or allies, but also that it doesn't appear to focus on those as well. And there's the challenge, as we develop interesting new active techniques, of how do you control single-point information. That is, information that is vital to you to being able to carry out offensive operations, but if it were known to an adversary, could make you very vulnerable as well. And finally, there are the problems that you usually don't have to worry about but General Minihan and I do have to worry about - that's the political issues: it's our image, it's getting caught, and it's on being the National Security Agency, not the National SIGINT Agency or the National INFOSEC Agency. It's all of the things that have to go together to make sure that we have, in fact, a future for all of you to be expert in.

"""""""

4. (U) KRYPTOS SOCIETY NEWS

(FOUO) The CSE Chapter of the KRYPTOS Society is Now Open for Business!
La Societe KRYPTOS, Section CST est prete pour les affaires!
By [redacted]

[N.B.: Canadian spelling and usage have been preserved throughout this article.]

(FOUO) As at NSA and GCHQ, there is a group of people at CSE that believe in the goals and purpose of the KRYPTOS Society: to promote interest in cryptanalysis; to provide a focal point for fields of common cryptanalytic interest; and to promote excellence in professional cryptanalytic activity in the cryptologic community. Having close ties with NSA and GCHQ in various activities, it was felt that establishing a CSE Chapter of the KRYPTOS Society would provide us with another means of exchange and forging closer ties with our community cousins. But more importantly, it would provide a means for people from the various groups at CSE to meet, share ideas and experiences, and forge closer professional relationships, all in the spirit of the KRYPTOS Society.

(FOUO) On March 21st of this year, the KRYPTOS Society reviewed and accepted our application for a Chapter at CSE. Our bylaws have been submitted to the NSA council for review and have been accepted! Thus as of June 21st, CSE has a Chapter of the KRYPTOS Society and we are now open for business!

(FOUO) Let me introduce to you the members of our Council:

President: [redacted]
Treasurer:
Secretary:
Newsletter Rep:
Programs Rep:
Consultant:

(b)(3)-P.L. 86-36

(U) We currently have two committees: one responsible for the Newsletter and the other for the Chapter's program of activities, and are looking forward to participating in the whole spectrum of KRYPTOS activities (e.g. the literature contest, the presentation contest, etc.) in the not-too-distant future.

(SC) To promote our Chapter and assist in its membership drive, we have alreadysponsored two highly successful talks. The first one was given by [redacted] during his visit to CSE in early June entitled: "South Africa: Out of the Closet". This was followed shortly thereafter by a talk by [redacted] who gave his perspective on how cryptanalysis and Sigint has evolved during his [redacted] years at CSE and where he believes they are going in the future as far as CSE is concerned.

(FOUO) Our program's committee have begun to look into scheduling future talks and showing of videos of talks originally given at NSA. Having integrees from NSA [redacted] and GCHQ [redacted] as part of the Council gives us the opportunity to be apprised of who is visiting CSE in the future and extending them an invitation to speak to our Chapter. Indeed, if you are visiting CSE and wish to give a talk to our Chapter,

(b)(3)-P.L. 86-36

[redacted]

you are more than welcomed to contact the respective integree, member of the Council or any member of the Program's committee: [redacted] or myself.

(U) It has taken a lot of work by a number of people to get our Chapter going, but based on the feedback I have received, there is a great deal of interest at CSE to participate in our Chapter, enjoy its sponsored activities and work with our counterparts at NSA and GCHQ by becoming involved in the various activities in the Society.

~~(FOUO)~~ And so in closing, speaking for the entire membership of our CSE Chapter, I would like to thank the KRYPTOS Society for approving our application which no doubt marked the beginning of a long and enjoyable partnership!

[redacted]

(b)(3)-P.L. 86-36

President of the CSE Chapter of the KRYPTOS Society

President de la Societe KRYPTOS Section CST

//

5. (U) TECHNICAL ARTICLES

(b)(1)
(b)(3)-P.L. 86-36

5a. ~~(FOUO)~~ Matt on Math
By [redacted]

[redacted]

[redacted]

(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

5b. ~~(FOUO)~~ Pete on PCS (b)(3)-P.L. 86-36
By [redacted] GCHQ Integree

(U) Why a PCS (or tour)?

~~(FOUO)~~ When I was first looking for a career out of college, one of the priorities high on my list was to work for a firm that offered opportunities to travel abroad. [redacted] (b)(6)
[redacted] Never one for short term gains at the expense of longer terms ones, I got my first tour after 12 years, just missing out on a couple of other tours

(b)(3)-P.L. 86-36

[redacted]

earlier in the '80s. After only 2 years back at GCHQ (the years I jokingly refer to as my TDY to GCHQ), I was fortunate to get my second, as an integree in Z Group. Most get their integrated tour first, but having done it the 'wrong' way round I feel that I have a better overview.

(U) Clearly a PCS is not for everyone. Personal circumstances and individual personalities are different. Some never PCS and some have had enough after one. For me the advantages shine through and I have yet to discover any real disadvantage, although being 'out of sight' >from one's parent agency may have short term career drawbacks.

(U) Even though it seems many things in the world are coalescing, much is thankfully still different. A PCS is a chance to see how another agency works (albeit will similar tools), exposure to different management techniques, structure and country. The settling in period is different for all; some people take 6 months, while I took about 24 hours! PCSers have to be self starters. At work and play one has to get out there and integrate, as the world will certainly not come to you.

(U) It can be a shock returning from a tour; after all you know how everything works, don't you? Not quite. In 3 years you have had experiences and changed slightly; so have the people and society you have been away from, and it is odd how one forgets some of the fundamentals of such life. It is also depressing that few are interested in your 3 years away and some seem to downright resent your good fortune.

(U) A PCS may not be for you or it may be with considerable thought. My nearly 5 years, to date, in the U.S. have been extremely pleasurable ones.

5c. (~~FOUO~~) Merits of Technical Diversification for Today's Problems
by [redacted] (b)(3)-P.L. 86-36

(U) Thanks to the KRYPTOS Society for giving me this opportunity to address you all and to reflect upon what is important to me, to the CA Community. It is an honor --and a challenge. At the moment I am not 'positioned' for a particular message. That is, I am not the Chair of any major cryptanalytic endeavor; work is predominantly compartmented in my current home. So, given free rein, I have chosen to reflect on how my particular flavor of diversified technical experience leads to optimism with the changing face of cryptanalysis today. Hopefully, this will paint an optimistic view in a general sense of such a career path, particularly to those of you starting out. At the risk of tedium, please bear with me for a synopsis of my past assignments.

N.B.: References to past offices use current designators, although most have changed since my tours.

(~~FOUO~~) I was hired decades ago, as a very green bachelors-degreed math major. During my first two months at NSA, two intern-program marketing talks, by CA star Virginia Jenkins and CA panel Chair Peter Jenks, sold me on the CA path. Both advanced the notion that with this choice you could take any tour you want and any course, go to graduate school and earn a masters, and then be equipped to solve almost any puzzle. Well, not quite, but there certainly were elements of truth

[redacted] (b)(3)-P.L. 86-36

here. In my initial assignment, the puzzle of straightforward depth reading was quite solvable and it gradually -as a rookie- occurred to me to pursue offices and tasks with more challenge, a way of life I continued well beyond intern graduation. [redacted] my last intern tour and only non-SIGINT one, became my permanent assignment as I finished my graduate degree in math after a one-year fellowship. [redacted]

(b)(3)-P.L. 86-36

[redacted]

~~(C-CCO)~~ I returned to the SIGINT world in the mid-80's. The first six years were in [redacted]

PCS (permanent change-of-station) at Center for Communications Research-Princeton came next. In this center of a few dozen cryptomathematical experts, I had the chance to hone skills in the areas of [redacted] such as [redacted]. Detours along the way include a co-chair of SCAMPs (Summer Conference on Applied Math Problems) in 1988 and '94, and a participant in SCAMP '96.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(FOUO)~~ My latest adventure is in Z03, where I endeavor to adapt past experiences to today's world. As I try to find a niche in this new world, similarities between new and old problems are increasingly apparent. I see cryptanalysis as very much alive, and present everywhere. My Webster's defines cryptanalysis to be "that act or science of deciphering codes or coded messages without a prior knowledge of the key." This definition supports that premise on the SIGINT side at least. INFOSEC crypt designers try to prevent, rather than enable, decipherment without the key. And it has been said that Julius Caesar invented the 'Caesar cipher ring' without using any cryptanalysis. But these days cryptanalytic techniques are germane to gaining confidence in the security of crypto design. Extrapolating from the Webster's definition, I consider that a coded message (like source 'code') is a set of bits we don't understand without key information and cryptanalysis is the science of turning that set, or some targeted portion of that set, into something we do understand. From this definition, we view cryptanalysis on many, new internet-related bitstream problems.

What are some familiar types of bitstreams? ~~(C-CCO)~~

[redacted]

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted] An 'engineering' experience that I considered an isolated incident then, 15 years later has application for many kinds of analysts in increasingly common environments.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Benefits of a diversified approach? (U)

1. (U) The primary one is that it diminishes the element of surprise when encountering new and different types of (software or hardware) data. So, it is easier to understand new problems in the context of old ones and to adapt applications of the past. --If your personality is like Garfield's, then there is no element of surprise in any case, but for myself changing offices has been a good way to nullify that very present element.

2. (U) It increases people networks;

3. (U) It reduces the effort of repeated learning curves like needed in adapting to new workstation environments, for example; and

4. (U) It is humbling.

Disadvantages? (U)

1. (U) It inhibits deep expertise in narrow fields. This may be a "bug or a feature", as they say, depending upon your perspective;

2. (U) There are many bureaucratic aspects -- procedures, policies, etc. -- which have little to do with the fun, technical aspects. These take time to learn, and the benefits seem marginal; and

3. (U) It is humbling -- definitely a bug and a feature!

(U) My main message is that, despite a few down sides, a diverse approach increases the likelihood of using what you learned to help solve diverse, new problems. Feeling more comfortable with today's challenges far outweighs the disadvantages I have come across from my particular method of diversifying. To you who are relatively new to NSA in particular, I encourage you to participate in various research efforts -pods, SCAMPs, etc. Unless you have a great sense of where to focus deeply and are very much committed to it, this time-of-flux seems like an excellent chance to develop cross-discipline skills in computer science, mathematics, cryptanalysis, engineering, signals analysis while gaining a useful understanding of a variety of problems facing crytpanalysts today. And if you think there is a need for a research center, push for it! Lean on your management. Rely on the CA community, panels, professional societies, enlighten groups, etc., for support to make this happen. Although it is not clear what tomorrow's challenges will be, it is certain that they will be different. From my perspective, this is a great way to prepare.

5d. (U) "Update and Revision of the Cryptanalysis Classification Guide" by [redacted]

[redacted]

(b)(3)-P.L. 86-36

(U) This article is reprinted from ENLIGHTEN.

(U) The Cryptanalysis Classification Guide has been revised and updated -- the new number is 342-97 -- it supersedes 342-95. Under the new classification guidelines, your "derived from" will be:

Derived from: NSA/CSS Classification Guide 342-97
Declassify on: X1, X5

~~(C-CCO)~~ The topics covered in this new guide are:

[redacted]

(U) The associated " Classification Facts for the Cryptanalyst" Classification Working Aid, 01-97, has also been updated to include all of the latest facts -- including those that have been recently declassified. This working aid is intended to help the cryptanalytic community in identifying what facts are classified, and where the fact was derived from.

(U) Both the Classification Guide (342-97) and the Working Aid (01-97) can easily be found on the Z Group WEB.

~~(FOUO)~~ If you have any questions relating to the classification guide or the working aid, please contact one of the Z Group Classification Advisory Officers.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

5e. [redacted]

by [redacted] Z and [redacted] R51

Background (U)

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(FOUO)~~ When the [redacted] group briefed DDO and DDT in February 1997, they proposed that two DO/DT teams be formed immediately. [redacted] was to plan the establishment of a production process while [redacted] looked at augmentation of the research process. The [redacted] proposal was approved by DDO and DDT, and by the end of February, [redacted] was named the Executive Agent of [redacted] with [redacted] and [redacted] named as the leaders of [redacted] and [redacted] respectively.

~~(FOUO)~~ The [redacted] teams have each drafted proposals and have begun to brief senior leadership, including DDO and DDT, on their recommendations. The proposals are summarized below, but it should be noted that these are draft recommendations: the details of their implementations are yet to be resolved.

[redacted] ~~(FOUO)~~

(b)(3)-P.L. 86-36

[redacted]

~~(S-CCO)~~ The [redacted] team began its effort by defining an overall [redacted] process model that differentiated research/technique development from production activities. This model outlined three separate activity threads - technique development, developmental exploitation (overlapped research/production), and sustained production exploitation. Four groups were identified to support the production portions of this process model: Customer-Focused Analysis and Development for customer liaison and target development; Operational Production for carrying out exploitation activities; Production Software Development to create and package software tools and databases to support Operations; and Infrastructure Development and Management to provide and manage the production hardware/software baseline. Given these groups and the process flow, an analyst-driven production cycle was identified and described along with a detailed list of the software tools, databases and hardware infrastructure needed to support it.

~~(S-CCO)~~ To reach the [redacted] goal of migrating the example projects

(b)(3)-P.L. 86-36

[redacted]

into a scalable, flexible, and sustainable production process, the following is recommended:

* Build the hardware infrastructure for exploitation operations in the OPS complex.

* Develop the production software tools and databases needed to support target development and [redacted] exploitation operations.

* Begin intensive training in [redacted] exploitation operations to expand the pool of qualified people capable of performing this function.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(C)~~ Resource estimates to build an initial production operations capability within a year are: [redacted]

resources will be provided by DO, the implementation details have yet to be worked out.

[redacted] ~~(FOUO)~~

~~(FOUO)~~ The [redacted] team consisted of [redacted] Technical Director, served as mentor. The team interviewed representatives of many Agency organizations to find out the current status of their research and to identify gaps in coverage of key technologies. Their proposal recommends specific actions for DO and DT.

(b)(3)-P.L. 86-36

~~(S-CCO)~~ In addition to the technology gaps, the team found several systemic problems that it termed "cultural gaps." Not all of these problems are unique to the [redacted] arena, but all are important. The two most significant gaps are (1) the lack of corporate operational goals for [redacted] exploitation and (2) [redacted]

~~(FOUO)~~ The Agency needs an aggressive 5-year corporate goal for the [redacted] contribution to the Agency product; the recommendation is [redacted] for the 1st quarter of 1997. Such a goal would galvanize the DO and DT commitments and it would provide focus and coordination to the research, development and production processes. [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(FOUO)~~ The heart of the [redacted] recommendation is a list of seven new research initiatives, each with a detailed research proposal. They are:

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted]

* ~~(C CCO)~~ [redacted] should be started. Some members of each pod should be designated from the start as those who will continue the pod efforts in their home branch [redacted] after the pod disbands, when the other pod members return to their organizations.

* ~~(FOUO)~~ [redacted] - The results of the [redacted] pod should be captured and continued by a permanent organization [redacted] when the pod ends.

* ~~(S CCO)~~ [redacted]

* ~~(S CCO)~~ [redacted] should be formed in the Fall to carry on the most promising research from the Bowie SCAMP. Again, this effort should be closely coordinated with the [redacted]

~~(FOUO)~~ In all, the [redacted] team recommends [redacted] new people be added to the research efforts before the end of the summer, with approximately [redacted] coming from Z. As noted above, the teams will be housed in different organizations. A technical oversight board composed of representatives from [redacted] will coordinate the teams' activities.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

"""""""

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TSUO)~~ The talks will probably not last 2 hours, but we have the room just in case :)
We hope to see you there!

[redacted]

** Calendar Appointment **

Date: 08/19/97
Start: 9:00 am
Stop: 11:00 am
What: Z2SP Student Presentations
Room 9A135

[redacted]

(b)(3)-P.L. 86-36

** Calendar Appointment **

Date: 08/21/97
Start: 9:00 am
Stop: 11:00 am
What: Z2SP Student Presentations
Room 9A135

[redacted]

6b.(U) NSA Science and Engineering Society Presentation

This article is UNCLASSIFIED in its entirety.

The NSA Science and Engineering Society will sponsor a presentation by [redacted] on August 14, at 10:00 AM in the Research and Engineering Symposium Center. The title of their talk will be:

"HYBRID TECHNOLOGY MULTI-THREADED ARCHITECTURE
FOR HIGH PERFORMANCE COMPUTING."

Many important problems in Physics, Chemistry, Biology, Fluid Dynamics, Cryptology, etc..require computation in the 100 Teraflop to 1000 Teraflop (Petaflop) performance range. Presently used architectures and hardware appear inadequate to achieve that goal in a timely, affordable, and credible way.

NSA has started a program with JPL to investigate the feasibility of a new architecture and its requisite hardware. The parallel processor configuration uses a multi-threaded architecture in order to accommodate the unavoidable latency of the memory path. To keep the

(b)(3)-P.L. 86-36

[redacted]

number of processors "small", less than 10,000, we are investigating the use of "single flux quantum" logic devices which are expected to operate at very low power and 50 Ghz, or faster, clock rates. Beyond that, the difficult speed and power requirements are overshadowed by the even more stressful requirements placed on the hierarchy of memories and the interconnections among them. These elements are also candidates for new technologies.

[redacted] is a research physicist in [redacted]. His field of specialization is Low Temperature Physics, with particular emphasis on high speed electronics and Superconductive devices. Much of his work has been applied in the area of high performance computing. He [redacted] (b) (6)

[redacted] has been a researcher at the IDA Center for Computing Sciences since 1990. His specialties include programming languages and compilers, systems architectures, operating systems, and distributed computing systems. [redacted]

This presentation is unclassified. All personnel are invited to attend. The presentation will be broadcast over Newsmagazine Channel 17.

~~(FOUO)~~ For information on or membership in the Science and Engineering Society contact Tom Kline, [redacted]

6c.(U) NSA Science and Engineering Society 1997 Call for Papers (b) (3)-P.L. 86-36

This article is UNCLASSIFIED in its entirety.

The NSA Science and Engineering Society announces the fourth annual Science and Engineering Technical Paper Contest. The purpose of this competition is to recognize outstanding written contributions to the science and engineering fields. It is hoped, in addition, that such recognition of written work will encourage the sharing of expertise and experience in science and engineering throughout the NSA community.

Authors must be employees of NSA or members of other cryptologic elements assigned duty at NSA HQ or field sites. Jointly authored papers are acceptable; winning teams will share the prizes. Papers in all science and/or engineering fields may be submitted. They may be classified up through the TSC/TK/[redacted] level (no compartmented papers accepted). Titles and abstracts must be classified appropriately for publication via NSA's WEBWORLD, ESS, and ENLIGHTEN. (For example, no TK or US ONLY titles or abstracts). Only papers written since 1 June 1996 are eligible. The manuscript must be no more than 50 pages in length, not including the coversheets described below. Papers published or accepted for publication in outside journals are not automatically excluded. However, since they may have been edited by technical referees or editors, only the author's draft, as originally submitted for publication will be accepted for this competition.

Up to three cash prizes for $250, $150 and $100 will be awarded to winners of this contest at the S&ES Fall luncheon. Plaques will also be given to each of the winning authors. If no papers are submitted which the judges deem worthy, no awards will be given. (b) (3)-P.L. 86-36

[redacted]

Papers will be judged on the following criteria:

1. Relevance to the science and/or engineering field
2. Significance of the content to the Agency mission
3. Interest of the paper to Agency professionals
4. Quality of writing
5. Originality
6. State-of-the-art

~~(FOUO)~~ Submission: Each author or team should submit one hard copy of the paper by 2 September 1997 to:
S&ES Technical Paper Contest Evaluation Committee,
[redacted]
Wayne E. Smith, Jr., [redacted] email: [redacted]
Further information on this S&ES Technical Paper Contest can be obtained from [redacted] or Wayne Smith on [redacted] or via email (preferable).

---

7. (U) LITERARY NOTES: Book Review

(b)(3)-P.L. 86-36

~~(FOUO)~~ _The Bible Code_ by Michael Drosnin -- Book Review by [redacted]

This review is UNCLASSIFIED in its entirety.

Some of our readers may already be aware of the Bible Code but the first time I heard of it was in a 15 June TV news report. The news report peaked my interest and Mike bought the book the next day. After reading it, I decided to share information from the book and some comments from the internet on the Bible Code with our _Tales of the KRYPT_ readers.

Initially Drosnin, an investigative reporter, went to Israel to meet with the Chief of Israeli Intelligence to research the future of warfare. While there, a young intelligence officer told him that he should see a mathematician in Jerusalem named Rips who had found a code in the Bible with the exact date the Gulf War would begin, three weeks before the war started.

Eliyahu (Eli) Rips is considered a genius in the world of mathematics. When Drosnin first visited Rips in Jerusalem in 1992, Drosnin picked up a Bible and asked Rips to show him the Gulf War. Rips didn't open the Bible but turned on his computer, telling the reporter that "The Bible code is a computer program." Hebrew letters highlighted in five different colors creating a crossword puzzle pattern appeared on the screen. A print-out showed that "Hussein", "Scuds", and "Russian missile" were all encoded together in Genesis. Eli had also found the date "fire on 3rd Shevat" which in the Hebrew calendar is equivalent to 18 January 1991 - the start of the Gulf War.

The Bible as it was first written -- the original Hebrew version of the Old Testament -- is where the Bible Code was discovered. Even though the Bible has been translated into every language, the Bible Code only exists in Hebrew. The first hint of the encoding was found more than 50 years ago by a rabbi in Prague, Czechoslovakia, who noticed that if he skipped fifty letters, and then another 50, and then another 50, the word "Torah" was spelled out at the beginning of the Book of Genesis. He found the same skip sequence again spelled out the word "Torah" in the Book of Exodus, in the Book of Numbers, and in the Book

(b)(3)-P.L. 86-36

[redacted]

of Deuteronomy. This "hidden text", as described by Rips and his colleague, Doron Witztum, a physicist, is composed of words spelled out by skipping equal numbers of letters through the original Hebrew text. They call this phenomenon Equidistant Letter Sequences (ELS).

Sir Isaac Newton, the first modern scientist, was obsessed with finding a hidden code in the Bible which would reveal the future. He learned Hebrew and spent half his life trying to find the code. The author notes that there was one essential tool that Rips had which Newton didn't - a computer. The author says "The hidden text of the Bible was encoded with a kind of time-lock. It could not be opened until the computer had been invented."

Rips and Witztum did a controlled experiment in the Book of Genesis >from which they found the names of 32 Jewish famous sages and their dates of birth and death. After a peer review by several mathematicians and more testing on "fresh" data, the experiment was deemed successful. An independent experiment to test the phenomenon was conducted by Harold Gans, a senior Cryptologic Mathematician now retired from NSA. Gans is described in the book as "a senior code-breaker at the top secret U.S. National Security Agency, who confirmed that there is a code in the Bible that does reveal the future." Gans initially was sure that the Bible Code was "off-the-wall, ridiculous." But after his own independent research, including writing his own program, he found the same information as Rips and Witztum. He then decided to see if the places of birth could be found and he did find them as well as 34 additional names of personalities. These results made him a believer. Most recently, Harold Gans issued a public statement via the internet which refutes Drosnin's theory of the Bible Code predicting the future.

Drosnin was initially skeptical about the code and could not believe the divinely inspired Bible held a meaningful and human-discernable secret code. Doing his own research on Hebrew text of the Old Testament using the program Rips showed him, Drosnin discovered an ELS set of remarks suggesting Yitzhak Rabin's assassination in 1994, one year before Rabin was killed. This convinced Drosnin of the validity of the code, a point driven home by Rabin's death in 1995. The jacket of the book prominantly displays the matrix window showing the name "Yitzhak Rabin" running down a column and the words "Assassin that will assassinate" intersecting on the row with the second letter of his name. After the assassination of Rabin, Drosnin found the name of the assassin, "Emir" near the original ELS associated with Rabin's assassination. Drosnin spent five years researching the Bible Code and this book is a result of his work.

Drosnin details consistent "findings" of modern events, such as the Oklahoma City bombing and the election of Netanyahu as Israeli Prime Minister - all encoded in the first five books of the Bible. His "findings" include such "translated" word patterns as "Bible Code" - "He encoded the Torah, and more." - "Sealed before God." Drosnin's "findings" also cover known assassinations from Abraham Lincoln to John F. Kennedy to Bobby Kennedy to Anwar Sadat with dates, places, and names of the assassins. For example, the "translated" word patterns he gives for the John F. Kennedy assassination are: "President Kennedy" - "To die" - "Dallas" - "Oswald" - "Marksman" - "Name of assassin who will assassinate" - "Oswald" (again) - "Ruby" - "He will kill the assassin." Drosnin tries hard to "predict the future" based on his version of the Bible Code. He provides "word patterns" to support his predictions about "an atomic holocaust" and the "End of Days."

(b)(3)-P.L. 86-36

9/24/2010

Unless you can read Hebrew, the many examples Drosnin gives in the book must be accepted "on faith." However, critics of the Bible Code, among the many Internet sites, accuse Drosnin of loosely translating Hebrew text to fit his objective. Mathematicians also argue that even Rips, outside of "wild" claims by Drosnin, arranges matrices to fit his "observed" ELS decodings.

The book was an interesting read once you got used to Drosnin's repetitiveness. But it would be unwise to call it scientific or anywhere near mathematically proven.

****
//////////

8. (U) PROBLEMS AND PUZZLES
by [redacted] Z433

8a. (U) Solution to July puzzle (courtesy of [redacted]

This puzzle is UNCLASSIFIED in its entirety.

Some months ago there was a puzzle about five pirates trying to divide up 1000 gold coins. This is an extension to that puzzle.

Once again we have five pirates, with the following six characteristics:

(b)(3)-P.L. 86-36

1) Will do anything to avoid dying
2) Infinitely bloodthirsty
3) Infinitely greedy
4) Smart
5) Risk neutral: e.g. a half a chance of getting 10 coins is no better or worse than certainly getting 5
6) They are all ambivalent to each other

They have a booty of 1000 gold coins to share, and reach the following agreement for doing it.

They will draw straws. The short one makes a proposal. Everyone votes. If a clear majority are in favor, the money is divided up. Otherwise, they throw him overboard (so he dies), and draw straws again.

What should the pirate who draws the short straw first propose?

Solution: (courtesy of [redacted]

As with the other problem, we'll work it back from 2 survivors. We shall call the one who draws the short straw at each stage, "Roger". We know that it is someone different each time but, since it is well-known that all pirates are called Roger, it doesn't matter.

With 2 survivors, Roger dies and the other keeps all. The expected winnings for each is 500 coins. Therefore if there are 3 pirates remaining, Roger needs to offer one of the others 501 coins in order to gain their vote. Obviously, the expected winnings of each is 1000/3 coins.

With 4 pirates remaining, Roger has to get the vote of at least two of the others, and so must offer them each at least 334 coins. He can therefore keep 332 for himself. Expected winnings are 250 coins.

(b)(3)-P.L. 86-36

[redacted]

For 5 pirates, Roger needs to offer 2 others 251 coins each but can keep 498 for himself.

Note that, we needn't have gone through all that analysis. We could have started with the fact that, with 4 pirates remaining, they will all use the same strategy if they draw the short straw so the expected winnings for each pirate is 1000/4 = 250.

Now consider N pirates. The expected winnings for (N-1) pirates is 1000/(N-1). Roger needs to get the vote of Floor(N/2) of the other pirates in order to survive, so he should offer each of them

1 + Floor(1000/(N-1)).

So he can keep 1000 - (Floor(N/2) * (1 + Floor(1000/(N-1))) coins himself.

If N>4 and not too big, this means he does better than his fair share!

Something startling appears to happen around N=1000 (but in fact occurs near every divisor of 1000)

# pirates	# coins for Roger
2	0
3	499
4	332
5	498
6	397
7	499
8	428
9	496
10	440
..	...
99	461
100	450
101	450
...	...
996	4
997	4
998	2
999	2
1000	0
1001	0
1002	499
1003	499

Solutions were received from [redacted]

8b.(U) August puzzle
(Taken with permission from the pages of the Grey Labyrinth at http://www.wx3.com/labyrinth/index.htm if you have an outside account).

This puzzle is UNCLASSIFIED in its entirety.

(b)(3)-P.L. 86-36

After spending several hours pouring over the puzzles in the Labyrinth, you work up quite a thirst. So you stroll down the hall to the company soda machine. The machine has three buttons, which dispense "Royal-Fizz-Cola", "Dyspepsia", and a third which randomly distributes

[redacted]

either one. Years of experience have shown that the labels are never correct. For example, the button labeled "Royal-Fizz-Cola" might always yield Dyspepsia, or it might randomly deliver either, but never reliably Royal-Fizz-Cola.

Today the machine was refilled, so you don't know which button gives which soda. If making a selection costs a dollar, what is the minimum you must spend, and why, before you can be certain which buttons deliver which sodas?

Send answers, as well as puzzle submissions, to [redacted]

[redacted]

9.(U) EDITORIAL CORNER

REMINDER: Submissions for the September issue are due by August 22nd.

PLEASE NOTE: All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

If you have any comments or suggestions, please submit them to any member of the editorial board.

(~~FOUO~~) EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

[redacted]

(b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

(b)(3)-P.L. 86-36

[redacted]

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

TOP SECRET//COMINT

(b)(3)-P.L. 86-36

[redacted]

TOP SECRET//COMINT

(U) POC: [redacted] info
(U) *Last Modified: 10/30/2002 11:42:23*
(U) PE EXTERNAL PAGE

```
**********************************
*        TALES OF THE KRYPT      *
**********************************
```

January 1998

```
////////////////////////////////////////////////////////////////////////////
****************************************************************************

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
////////////////////////////////////////////////////////////////////////////
```

(U) TABLE OF CONTENTS:

1. (U) Calendar of Events

2. (U) Word from the CACP:

   2a. (U) CA PQE Update

   2b. (U) Intern Accomplishments

   2c. (U) Calling All Senior Cryptanalysts

3. (U) KRYPTOS Society News: Fourth Annual BANCC for Newly Certified Cryptanalysts

4. (U) Technical Article

   (FOUO) "How I Met the `Bit Fairy'", by [redacted] CMP Intern

5. (U) Community News

   5a. (U) Upcoming Annual Cryptomathematics Exchange (ACE)

   5b. (U) Cryptanalytic Software Conference 1998 (CRYSCO '98) Call for Papers

   5c. (FOUO) Sir Peter Marychurch Awardees Announced:
   [redacted]
   (Reprint of Announcement by [redacted]

6. (FOUO) CA History: "The _Lusitania_ and British Cryptanalysis", from _CRYPTOLOGIC ALMANAC_, by [redacted]

7. (U) Recommended Reading: "Collected Papers on Cryptanalytic Diagnosis", from _NSA's Attic_

8. (FOUO) Problems and Puzzles by [redacted]

9. (U) Letter to the Editor

   (FOUO) "Some Things Never Change"

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

by [redacted]

10. (U) Editorial Corner (b)(3)-P.L. 86-36

****
//////////

1. (U) CALENDAR

Jan 29 (U) Fourth Annual Breakfast Affair For Newly Certified Cryptanalysts (BANCC), 0800-1000, Canine Suite (See 3a.)

PLAN AHEAD

Mar 23-27 (U) CARD '98 at CSE

Mar 30-April 3 (U) CRYSCO at NSA (See 5b.)

Apr 13-17 (U) CA-305 at NSA

Apr 20-24 (U) Signals Analysis Development Conference

May 11-15 (U) ACE at GCHQ (See 5a.)

****
//////////

2. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

2a. (U) CA PQE Update

~~(FOUO)~~ The CA Career Panel has made some changes to the eligibility requirement for taking the annual Professional Qualification Examination (PQE). Instead of having to complete two years of cryptanalytic work experience and approximately eight training courses, the aspirant must now complete one year of CA experience (two of the five diversity tours), and three courses: CA-107 (Exploitation of Manual Cryptosystems), CA-123 (Introduction to Shift Registers), and CA-110 (Introductory Cryptostatistics). The new requirements were instituted in an effort to afford the aspirant more opportunities to attempt the PQE.

(U) The PQE will be given in early May; announcements of dates, sign-up procedures, and review sessions will be made in future editions of _Tales of the KRYPT_, as well as on ESS topic 1284, and via wide email distributions.

2b. ~~(FOUO)~~ Intern Accomplishments

The Cryptanalysis Career Panel is pleased to announce the following:

[redacted] - Promotion to GG-13

[redacted] - SPCA

[redacted] - SPCA (b)(3)-P.L. 86-36

[redacted]

2c. (~~FOUO~~) Calling All Senior Cryptanalysts

Are you looking for a career-enhancing way to serve your skill field? The Cryptanalysis Career Panel (CACP) is now accepting applications for Panel membership. The CACP addresses issues dealing with the cryptanalysis career field, such as professionalization, technical track oversight, CA intern and cross-training programs, hiring, annual cryptanalysis conference, CA training, and other matters. Panel members are expected to attend monthly meetings and participate in working groups or subcommittees related to the above issues. Professionalized cryptanalysts (Grade 14 and above) from all over the Agency are invited to apply. To submit an application, email a current PERSUM and narrative paragraph stating why you would like to join the Panel and what you feel you could contribute, to the CACP office (h111aaa2nsa) by COB 2 February 1998. For more information call [redacted]

//

3. (U) KRYPTOS SOCIETY NEWS: Fourth Annual BANCC for Newly Certified Cryptanalysts

(U) The KRYPTOS Society is pleased to announce the Fourth Annual Breakfast Affair for Newly Certified Cryptanalysts (BANCC).

(~~FOUO~~) List of Honorees:

[redacted] (b)(3)-P.L. 86-36

(U) WHEN: Thursday, January 29, 1998
8:00 to 10:00 a.m.
Breakfast Buffet is scheduled to be ready by 8:00!

WHERE: Canine Suite

COST: $6.00

Breakfast Buffet Menu:
Traditional Scrambled Eggs
Crisp Bacon
Sausage Links
French Toast
Homemade Biscuits
Hash Brown Potatoes or Cinnamon Apples
Juice
Selection of Teas
Freshly Brewed Coffee

(b)(3)-P.L. 86-36

[redacted]

(FOUO) Sign up and pay $6.00 to one of the following people by Monday, January 26, 1998:

[redacted] (b)(3)-P.L. 86-36

(FOUO) If you have any questions regarding this breakfast, please contact [redacted]

//

4. (U) TECHNICAL ARTICLES

(FOUO) How I Met the "Bit Fairy", by [redacted] CMP

(FOUO) I am a Z group cryppie. As such, there is a seemingly endless supply of bits to analyze. Sometimes I am successful, other times I'm not. I never really gave any thought, however, to where the bits came from or how they came to be in my directory tree... until now.

(U) Most readers are familiar with baseband digital systems, where digital ones and zeros are transmitted directly without any shift in the frequencies. Because these signals have high power at low frequency, it's perfectly natural to send these over a pair of wires or a length of coaxial cable. These signals, however, cannot be transmitted over the air because you would need an antenna the size of the World Trade Center in order to radiate the low frequency spectrum of these signals. In order to transmit these signals over a radio link we must shift the signal's frequency spectrum--modulate the signal--to a higher band.

(U) The spectrum of a baseband signal can be shifted to a higher frequency by modulating a high frequency sinusoid--carrier--by the baseband signal. Consider a general sinusoid or carrier

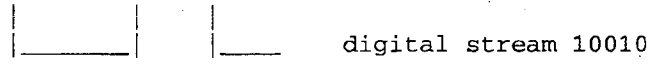
$$A*\cos(w*t + p)$$

it has three components: the amplitude A, frequency w, and phase p which may be a non-constant function of time t. Consequently, three basic types of modulation exist: amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM).

(U) In AM, the carrier's amplitude is varied in direct proportion to the baseband signal. For example, if our baseband signal is a stream of ones and zeros then the modulated carrier would look like short bursts of the

[redacted] (b)(3)-P.L. 86-36

[redacted]



carrier cos(w*t) when the baseband signal was a one and zero otherwise. This modulation scheme for transmitting binary data is known as on-off keying (OOK) or amplitude shift keying (ASK). You might think of OOK/ASK in terms of old Morse code transmitters and a data clock: When the key is pressed, we send a tone (binary 1), otherwise we send nothing (binary 0).

(U) In PM, the carrier's phase is modified according to the baseband signal. Recall the following identity from trigonometry:

$$\cos(A + B) = \cos(A)\cos(B) - \sin(A)\sin(B).$$

Using this identity we see

$$\begin{aligned}\cos(w*t + pi) &= \cos(w*t)\cos(pi) - \sin(w*t)\sin(pi)\\ &= \cos(w*t)\ (-1) - \sin(w*t)\ (0)\\ &= -\cos(w*t).\end{aligned}$$

Hence, we can transmit a binary 1 by cos(w*t) and a binary 0 by -cos(w*t). These signals are out of phase by 180 degrees. Clearly, in phase shift keying (PSK) the digital information is carried in the phase of the carrier.

(U) Finally, in FM, digital data is transmitted by varying the frequency of a carrier. In the case of frequency shift keying (FSK) a binary zero is transmitted by sending cos(w_0*t) and a binary one is transmitted by sending cos(w_1*t) where w_1 > w_0. One might think of FSK in terms of a piano keyboard. To transmit a zero, we hit the (say) low A key; to transmit a one, we hit the (say) high F key.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

"""""""

CCR-LJ, CCR-P, and CCS.

(FOUO) Each afternoon will be split into 3-5 parallel workshops, each workshop on a single topic. The intent is to keep workshops open to as many attendees as possible. However, [redacted] sessions will be considered if they allow for the exchange of useful new ideas across the cryptomathematics community.

(S-CCO) Among the topics to be featured at this year's conference will be sessions on:

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(FOUO) Abstracts may be up to 8 pages in length and must be properly classified, including paragraph classifications. Note that in a change from last year, "final" abstracts are being requested at the beginning of the selection process. All abstracts should be submitted through a local ACE representative by 23 January.

(FOUO) US personnel must also submit a signed Conference Approval Sheet (available from ACE reps) by the above date directly to [redacted] Forms may be forwarded via secure fax to [redacted] weekdays, 6am - 8pm, "for [redacted]

(FOUO) ACE representatives:

[redacted]

(b)(3)-P.L. 86-36

(U) Remember that abstracts for proposed ACE98 talks are due by 5 pm FRIDAY, JANUARY 23.

5b. (FOUO) Cryptanalytic Software Conference 1998 (CRYSCO '98) Call for Papers

(C) The Cryptanalytic Software Conference 1998 (CRYSCO '98) will be held from March 30th through April 3rd 1998 at NSA. The theme of this year's conference will be: "Improving the Effectiveness and Availability of Analytic Tools." The purpose of this conference will be to facilitate software exchange, coordinate joint efforts, discuss future trends, and share experiences and express concerns over software

(b)(3)-P.L. 86-36

[redacted]

and software development issues. This conference will be attended by representatives of all Second Party agencies, and IDA contractors.

(U) The format of CRYSCO '98 will generally follow tradition. There will be a mixture of technical and liaison issues presented in the form of a discussion session. Nominally, discussion sessions will begin with a 10-15 minute briefing introducing the topic, and will conclude with approximately 70 minutes of moderated discussion with the amount of time allocated for the moderated discussion being adjusted according to the complexity of each session.

(U) The topics to be discussed at CRYSCO '98 are:

(U) How to use the Web and other information technology tools (e.g., CORBA).

~~(FOUO)~~ Microcomputer Architectures (Windows 95/98/NT, Linux, etc.) - How can we use them?

~~(FOUO)~~ The Software Engineering Institute's Capability Maturity Model - What is it and how can it deliver better software for the analyst?

~~(FOUO)~~ Object Oriented Methodology (OO) - How can we best use this? Which applications have been successful? Which have not?

~~(FOUO)~~ Cryptologic Infrastructures: Unified Cryptologic Architecture (UCA), SINEWS, etc. - What does it mean to developers/users?

(U) UNICODE short discussion session (10-15 minutes presentation, 30-35 minutes discussion).

(U) SMIRE Topics:

(U) How to retire programs.

(U) Managing change in software components (e.g., changing I/O of library routines) - how to do it without upsetting the apple cart.

(U) Commercial software - what we use, what we plan to use, and for what applications.

~~(FOUO)~~ Common operating environment for Z workstations.

~~(FOUO)~~ Handling dependencies in software - consequences for package librarians, and exchange issues.

~~(FOUO)~~ Software Exchange Issues

~~(FOUO)~~ Defense Information Infrastructure Common Operating Environment.

(U) New business

~~(C-CCO)~~ Modern Communications Software: Signals Analysis and Computer-to-Computer Communications:

What is being done?

(b)(3)-P.L. 86-36

What software is being used/developed?

Are there any unmet needs?

(U) Open discussion on programming topics/techniques - programmer's roundtable discussion.

What language(s) to use for a particular job.

Optimization vs. Portability.

To write scripts or programs.

Parallel vs. Vector vs. Distributed processing.

Other topics as appropriate.

(U) The Future of Computers:

SNV2 - What is it?

MPPs - Will the T3E ever work right?

Distributed Computing - I have a Cray-1 on my desk; what should I be doing with it?

(U) Liaison Topics:

CA Web Issues.

Year 2000. What problems are in the software? What is being done about them?

Should we hold any subject-specific liaison workshops?

What are our plans vis a vis the "next" generation of workstations - what are we looking for, what will we use?

(~~FOUO~~) Questions may be addressed to the following:

[redacted]

5c. (~~FOUO~~) Sir Peter Marychurch Awardees Announced:

[redacted]

(Reprint of Announcement by [redacted]

(~~C-CCO~~) It gives me great pleasure to announce that the recipients of the ninth annual Sir Peter Marychurch Award for excellence in cryptanalysis are [redacted] both of R51, for their remarkable accomplishments in discovering and developing a [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

(~~C-CCO~~) The Joint US/UK Selection Board described this work as follows:

[redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

//

6. (~~FOUO~~) CA History: "The _Lusitania_ and British Cryptanalysis", from _CRYPTOLOGIC ALMANAC_, by [redacted] (b)(3)-P.L. 86-36

(U) On 7 May 1915, within sight of the coast of Ireland, German U-boat U-20 struck the luxurious passenger ship _Lusitania_ with a single torpedo. The ship sank in eighteen minutes, killing 1,195 of the 1,959 passengers and crew, 123 of whom were Americans. Anger exploded on both sides of the Atlantic as the result of the incident. How could the Germans have been so barbaric as to sink a passenger ship? Could it have been prevented? Looking back on the event from almost eighty-three years in the future, we might find it odd that more steps were not taken to try to prevent such an attack. The British Admiralty's code-breaking organization had an ambitious cryptanalytic effort against the German Navy. Why did they neglect to warn the _Lusitania_ of the U-boat activity off the section of the Irish coast toward which it was heading?

(U) The British code-breaking organization, known as Room 40, was formed in August 1914. By late 1914, thanks to careful cryptanalysis and traffic analysis, Room 40 had learned a great deal about the German U-boat fleet, including its size and composition and the general location of each boat. In spite of this detailed information, it was impossible for the Room 40 analysts to know the precise location of any single U-boat at any given time. The exact location of each boat depended a great deal upon the weather, the availability of ships to attack, and the whims of the U-boat captain, none of which could be predicted in advance. So even if, for example, Room 40 knew that U-20 had been ordered to the Irish Channel in early May 1915, they would have had no idea where the boat was once it got there.

(U) Further complicating matters was that the Room 40 analysts had no idea where any British ships were. To attempt to protect British and Allied ships from German attacks, their exact locations were kept secret once the ships left port. The locations of the civilian ships were compiled and maintained by the Trade Division of the British Admiralty, which was not privy to Room 40's U-boat information, also for security reasons. Furthermore, the only man who appears to have had access to both sets of information and the power to take action to try to prevent the _Lusitania_ disaster was the First Lord of the Admiralty, Winston Churchill. Unfortunately, he was in France at the time, meeting with the commander of the British Expeditionary Forces and thus was unable to review the closely guarded decrypts of the German U-boat communications.

(U) So was the _Lusitania_ disaster caused in any way by Room 40's negligence? Definitely not. A paranoia for secrecy appears to have been the only serious flaw in the handling of the information derived from the decrypts at the time of the sinking of the _Lusitania_. This flaw, however, was not the fault of the Room 40 staff, but of their

(b)(3)-P.L. 86-36

[redacted]

superiors. Because so many people were ignorant of the very existence of Room 40, including the head of the Trade Division, Room 40's valuable information could not be used to its greatest advantage in warning civilian vessels. As a result of the sinking of the _Lusitania_, information from the decrypts was used to help British destroyers search out and sink U-boats, thus protecting all British shipping.

(U) Sources:

Ballad, Robert D. _Exploring the Lusitania_. New York: Madison Publishing Inc., 1995.

Beesley, Patrick. _Room 40_. London: Hamish Hamilton LTD, 1982.

"""""""

(b)(3)-P.L. 86-36
(b)(6)
(b)(7)(C)
(b)(7)(E)
OGA
FBI

(U) All,

(U) I'd like to share something with you.

[redacted]

(FOUO) [redacted] We talked about what has made him so successful in his job. He said, "Do you remember when we all had to take CA-111, [redacted] He then said, [redacted] told us that the first thing we should do is actually look at the data. After we decide what we want to do with it, we are to look at the data again. After we run tests and examine the results, we look at the data again. The key to my success is remembering and doing what [redacted] said -- 'Look at the data'."

(b)(6)

(b)(3)-P.L. 86-36

(U) My conversation with Mike brought back a lot of memories, but more importantly, it reminded me of the most important and basic rule of CA. You might say, "But isn't this just common sense for the CA?" It is, but how often do we forget to do it? CA-111 isn't taught anymore and I wonder how many new cryptanalyts have not heard these words of wisdom. I also wonder how many of us seasoned cryptanalysts have forgotten the rule. This email is just a friendly reminder.

(U) We have been very successful in cryptanalysis over the years and one of the reasons why is because we take the time to look at the bits. Technology has changed and continues to change, but the first step remains - we need to look at the data.

Thanks for taking the time to read this email.

[redacted]

(b)(3)-P.L. 86-36

(U) Editor's note:

(FOUO) In addition to [redacted] some other sources of the CA maxim of the value of actually looking at the data are Lambros Demetrios Callimahos in CA-400, and [redacted] in CA-212. Perhaps our readers can cite some others, or would write to _Tales of the KRYPT_ to expand on this theme.

//

10.(U) EDITORIAL CORNER

REMINDER: (U) Submissions for the February issue are due by January 22.
PLEASE NOTE: (U) All submissions must be in ASCII format, and, with the

(b)(3)-P.L. 86-36

[redacted]

implementation of E.O. 12958, MUST BE PORTION-MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted] (b)(3)-P.L. 86-36

[redacted]

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2, DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR" DATE OF SOURCE: 3 SEP 1991

[redacted]

(b)(3)-P.L. 86-36

[redacted]

~~TOP SECRET//COMINT~~

~~(C)~~ POC:

(U) *Last Modified: 10/30/2002 11:42:23*

(U) PE EXTERNAL PAGE

```
**********************************
*        TALES OF THE KRYPT      *
**********************************
```

February 1998

```
////////////////////////////////////////////////////////////////////////////
****************************************************************************

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
////////////////////////////////////////////////////////////////////////////
```

(U) TABLE OF CONTENTS:

1. ~~(FOUO)~~ Perspective: Text of Remarks at the Annual Breakfast Affair for Newly Certified Cryptanalysts (BANCC), by [redacted] D/Chief Z4, Chairman of the Cryptanalysis Panel

2. (U) Calendar of Events

3. (U) Word from the CACP:

   3a. (U) CA PQE

   3b. (U) Gold Bug Award

4. (U) KRYPTOS Society News: 1998 Membership Information

5. (U) Technical Articles

   5a. ~~(FOUO)~~ Matt on Math: "Factoring" by [redacted] CMP

   5b. ~~(C-CCO)~~ "[redacted]- A Case Study", by [redacted] GCHQ

   5c. ~~(FOUO)~~ An Evaluation of "The Bible Code", by [redacted]

6. (U) Community News

   6a. ~~(FOUO)~~ Cryptologic Mathematician Program (CMP) News, by [redacted]

   6b. ~~(FOUO)~~ Computer Communications Analysis Center Established (Reprint of Announcement by [redacted] Chief Z6)

   6c. ~~(FOUO)~~ Letter to All Z Technical Library Users, by [redacted]

7. ~~(FOUO)~~ Problems and Puzzles by [redacted]

   7a. (U) Answer to December KRYPTOS Kristmas Kwiz

   7b. (U) February Puzzle

8. (U) Letter to the Editor

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

(FOUO) "More about Looking at the Data" by [redacted]

9. (U) Editorial Corner

//

1. (FOUO) PERSPECTIVE - Each month this newsletter features the perspective of a Senior on a topic of his/her choice. This month we are pleased to publish the text of [redacted] remarks at the Breakfast Affair for Newly Certified Cryptanalysts (BANCC). Mr. [redacted] D/Chief of Z4, was speaking in his capacity as Chairman of the Cryptanalysis Career Panel.

29 January, 1998 BANCC Remarks:

(b)(3)-P.L. 86-36

(U) It is always a pleasure for me to participate in this breakfast where we salute those certified in cryptanalysis during the past year.

(U) A few days ago I was interviewing some people for the CACP Exec position. One of the candidates expressed some concern that the job would take her out of the technical mainstream. It reminded me of accepting my first team chief position. One really does go through "technical withdrawal"; you have the feeling that you are not getting nearly as much done as you used to. If your career progresses along this path, you must learn to derive satisfaction from what your group is accomplishing. It strikes me that there is a similar situation regarding the Exec position and all of us who devote time in service of the career panel. We, rightfully, derive satisfaction when analysts are certified, not only in what you have accomplished, but (perhaps more so) what you will accomplish. It's the old teach-a-person-to-fish analogy. Once taught, great things will happen.

(FOUO) And great things need to happen. I heard a technology forecast briefing the other day for UCA, the Unified Cryptologic Architecture (UCA). The UCA is NSA's initiative to cope with the rapid technological advancement that is all around us and affecting us in a myriad of ways. The briefing is one in which many of the graphs we ought to be concerned about have lines with steep slopes; there is a lot of sucking of air, "oh fudge", etc. From the cryptanalyst's perspective I don't think anybody believes that we are in a period of transition moving toward a point where technology will settle down and we will be comfortable again. Not at all. No, we are in a period of transition moving to a point where we, the analysts, will change; we will grow; we will be different; and we will regain comfort only if we are different from today. We will develop the tools and expertise that will allow us to be comfortable in an environment of constant change. The constant change is not going away. It's the new playing field; it's the hand we are dealt. I like to quote a statement made at a Z strategy session about a year ago, namely that "we (NSA's cryptanalysts) have to be able to move with the speed of business" -- for which products are turning over on the order of every six months. Our targets are operating in that environment. The data of interest to us is changing with that regularity. We must adjust, and, more than adjust by upgrading our tools, we need to continually upgrade ourselves. That is becoming a much more formal Agency goal, with structures in place to ensure it, structures that affect career advancement --- things like Tech Track, STDP, Tech Health awards, more active and influential THABs, etc.

(b)(3)-P.L. 86-36

[redacted]

(U) One aspect of these newer initiatives that you probably heard about is that professionalization may go away. You might think that a strange topic to bring up at this occasion where we are celebrating your certification. But we are not celebrating the piece of paper you received; we are celebrating the skills you have acquired. And THAT requirement won't go away. It may move to another part of the bureaucracy but it won't go away -- because cryptanalysts need these skills to meet the challenges ahead. And it doesn't stop with what is now the certification level. It's a career-long process.

(U) I believe that the need for ongoing technical development of every cryptanalyst is so intense that it has in fact become a paradigm shift, a new way of doing business, a new way of looking at things. That may sound strange in that the Agency has always encouraged such development, but I think the degree of need has taken it to a new level. Because of the constant turnover in technology, without a parallel CONSTANT advancement of our personal skills, we won't survive; we won't be able to do our job.

(b)(3)-P.L. 86-36

(FOUO) It is incumbent on each one of us to regularly take stock. [redacted] (Chief, Z4) advocates that everyone take the mirror test: look at yourself in the mirror and ask, "what do I see?" Do you see a cryppie? Do you see a manager? Do you see a technical leader? What do you see, now and for the future? Whatever we see, each of us ought to take that as a starting point/backdrop/impetus for career decisions. Or, put another way, NO move should be made that isn't purposeful and forward thinking. And I would add an additional question to the regular (monthly?, quarterly?) dialog we have with ourselves: what do I need to learn? --- to remain fresh, on top of things, what do I need to learn? What do I need to read? What courses do I need to take? What courses do I need to teach?

(U) So, congratulations. We do celebrate what you have accomplished and what you will accomplish. We celebrate what you have learned and what you will learn and what you will do to ensure that others learn. I recently heard a description of an unhealthy organization as being like a football game in which you have 22 people desperately in need of a rest being watched by 22,000 people desperately in need of exercise. Cryptanalysis is reasonably healthy in that regard; we have reasonably good participation from the community in efforts to keep CA healthy. I welcome you as professionalized members of that community and I encourage you to exercise.

(FOUO) BANCC Honorees:

[redacted]

(b)(3)-P.L. 86-36

//

2. (U) CALENDAR

[redacted]

Feb 20	(U) Deadline for submitting CA PQE questions. (See 3a.)
Feb 20	(U) Deadline for qualifying for a chance to win a Borders Gift Certificate by joining the KRYPTOS Society for 1998. (See 4a.)

PLAN AHEAD

Mar 23-27	(U) CARD '98 at CSE
Mar 30-April 3	(U) CRYSCO at NSA
Apr 13-17	(U) CA-305 at NSA
May 11-15	(U) ACE at GCHQ
Jun 4	(U) CMI Mathfest at R & E Symposium

//

3. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

3a. (U) CA PQE

(FOUO) Would you like to be immortalized? You have the chance to take part in creating the 1998 Cryptanalysis PQE (Professional Qualification Exam). The CA PQE Committee is now accepting questions for the upcoming exam, to be held in May. The questions may be either objective or narrative in style, and should be written so that an aspirant can answer them within half an hour without using a computer. The questions do not have to be polished (although it helps), but be sure to provide an answer, along with a brief explanation of the solution. Questions should be forwarded via encrypted email to [redacted] by COB 20 February 1998. Framemaker versions are preferred, and questions will be accepted from all sources.

(b)(3)-P.L. 86-36

3b. (U) Gold Bug Award

(U) The Cryptanalysis Career Panel is currently accepting nominations for the Gold Bug Award and the Gold Bug Team Award. The Gold Bug is an honorary award created by the Cryptanalysis Career Panel in 1982 to recognize outstanding technical excellence and achievement in cryptanalysis. While there is no particular time of year that the award is given out, the CA Career Panel is taking this opportunity to encourage all supervisors who have an employee or employees who might merit this distinction to submit their names and a description of their accomplishment. For more information contact the CA Career Panel on [redacted] or at h111@nsa.

//

4. (U) KRYPTOS SOCIETY NEWS: 1998 Membership Information

(b)(3)-P.L. 86-36

[redacted]

(U) Are you interested in cryptanalysis?
Do you like to see technical excellence encouraged and rewarded?
Would you like the chance to double your money?

If so, for just $5, you can join KRYPTOS for 1998 and possibly win a $10 gift certificate for Border's Bookstore!

(U) The KRYPTOS Society was established in 1981 to promote interest in cryptanalysis, to provide a focal point for the fields of common interest to cryptanalysts of the National Security Agency, and to promote excellence in the cryptologic community. For more information - see the KRYPTOS homepage at [redacted]

(~~FOUO~~) To join, please take $5 to one of the following friendly and helpful people, and fill out a short form at their desk:

[redacted]

(~~FOUO~~) Of the people who have joined by Feb 20, 15 lucky people will receive gift certificates! If you prefer, please fill out the following and mail along with $5 to [redacted]

[redacted] (b)(3)-P.L. 86-36

Name:
Organization:
Room Number:
Email Address:
Interested in chairing a committee? ____ Yes ____ No
Interested in working on a committee? ____ Yes ____ No
Check committees of interest to you:

___ Cryptanalytic Literature
___ Distinguished Members
___ Awards
___ Newsletter
___ Social Events
___ Membership
___ Publicity
___ Programs
___ Retired Members

//

5. (U) TECHNICAL ARTICLES

5a. (~~FOUO~~) Matt on Math (b)(3)-P.L. 86-36
by [redacted] CMP

(~~C-CCO~~) Most people who know me personally and professionally know that I am very interested in prime numbers [integers greater than 1 that cannot be evenly divided by any positive integer except 1 and itself] and factoring [writing non-prime or composite numbers as a product of

[redacted]

prime numbers]. The security of the Cocks-RSA public key cryptosystem [_Tales of the KRYPT_, April 1996] lies in the difficulty of factoring large composite numbers N into a product of two primes N = p * q. Recently someone asked me why we don't just generate all possible 512-bit Cocks-RSA numbers and use a look-up table to factor them. This month we will provide the reader with the tools to answer that question.

(U) Because large numbers have more potential divisors, primes become more sparse when we look for them among large numbers. If we look, we can see that there are arbitrarily large gaps between large primes. Observe that for any number n, the numbers (n! + 2) through (n! + n) are composite [recall that n! = n * (n-1) * (n-2) * ... * 1]. This is true because n! is divisible by all numbers from 2 through n. Thus, for k <= n, (n! + k) is the sum of two multiples of k and hence is itself a multiple of k.

(U) Since we can find an arbitrarily large gap between prime, a person might suspect that beyond some point there are no more prime numbers. This isn't the case at all. Euclid proved by contradiction that there are in fact infinitely many prime numbers.

> Suppose there are only a finite number of primes. We can write them down:
>
> p_1, p_2, ..., p_n.
>
> Consider the integer obtained by multiplying all the primes together and adding 1:
>
> E = (p_1 * p_2 * ... * p_n) + 1.
>
> This very big number E is one more than a multiple of p_i for any value of i between 1 and n. This E is not evenly divisible by any prime on our list (and that's all of them by assumption!) so E must be prime itself. Since E is much larger than any prime on our list, this contradicts the assumption that there are only a finite number of primes.

(U) We just saw that prime numbers are not regularly distributed. We can find primes like 17 and 19 that differ by two ["twin" primes] or we can show the existence of primes that are at least 10^99999999999 apart [using the factorial trick and the infinitude of primes]. The "prime number theorem", however, says that there is some regularity to their distribution. Let's address the question of how many primes are there in a given range of numbers. For example, how many 256-bit primes are there? The function pi(x) is traditionally used to denote the number of primes below (and including) the number x. For example, pi(1000) = 168 because there are 168 primes <= 1000. In his teens Gauss estimated the value of pi(x) to be x/log(x). Let's see how accurate his estimate is:

x	pi(x)	Gauss	pi(x)/(x/log(x))
1000	168	145	1.158
10000	1229	1089	1.128
100000	9592	8696	1.103
10^6	78498	72464	1.083
10^9	50847478	48309185	1.052

(b)(3)-P.L. 86-36

not too shabby! The estimate gets better and better as we take x larger and larger. In fact, about a century after Gauss formulated his estimate, it was proved that the ratio

pi(x) / (x/log(x))

tends to 1 as x tends to infinity. In other words, the "prime number theorem" states that considering large enough values of x the ratio can be made as close to 1 as you want. There are several refinements of Gauss' formula that provide better estimates for small values of x but they lack the elegance of Gauss' original formulation.

(U) HOMEWORK: Estimate the number of 256-bit primes.

Let x=2^256-1, the largest number that can be represented by 256 bits. Then, Gauss' estimate for the number of primes below x (i.e., all the primes including the 256-bit primes) is

A = x/log(x) = 1.50255 * 10^75.

Now let y=2^255-1 (the largest number that can be represented by 255 bits). The estimate for the number of primes below y is

B = y/log(y) = 7.54222 * 10^74.

Finally, we can estimate the number of 256-bit primes to be the difference of A and B above:

There are about 7.48329 * 10^74 256-bit primes.

Suppose we could store each of these primes in an atom. Since there are only about 10^67 atoms in our galaxy we are out of luck. Not to worry, there are about 10^77 atoms in the universe (excluding dark matter). So, now the only question left to answer is what do we do with the projected surplus?

5b. [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

[redacted] (b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

5c. (~~FOUO~~) An Evaluation of "The Bible Code"
by [redacted] (b)(3)-P.L. 86-36

(U) Editor's note:

(~~FOUO~~) The August 1997 issue of _Tales of the KRYPT_ featured a book review by [redacted] Chief Z609, of _The Bible Code_, by Michael Drosnin, New York: Simon & Schuster, 1997. At the request of the KRYPTOS Society, [redacted] CMP Program Director, has cryptanalytically evaluated the code itself.

(U) Let me spare you any anticipation or concern: I was completely unconvinced by _The Bible Code_; I did not like the book. It reminded me very much of other pseudo-scientific books I've read. For example:

-Erick Von Daniken's _Chariots of the Gods_ found evidence of extraterrestrial visitors in ancient legends, myths, and carvings around the world;

-Ignatius Donnelly's _Atlantis: The Antediluvian World_ told us all about the lost continent and its culture;

-E. Raymond Capt's _The Great Pyramid Decoded_ discovered all sorts of wondrous predictions in the dimensions and ratios of the great

[redacted] (b)(3)-P.L. 86-36

pyramid;

-Richard Noone's _5/5/2000: Ice the Ultimate Disaster_ warned of a planetary alignment on 5 May 2000 whose combined gravitational pull on the polar ice caps will change Earth's axis of rotation (and ancient Egyptians warned future generations of this in the dimensions and alignment of their pyramids).

(U) All of these books share many things in common, beyond a naive credulity. They are generally well-written, or at least easy to read. Their conclusions are gripping and challenge current thinking--in many cases they challenge the very foundations of our world view. And they all betray sloppy thinking and a general misunderstanding of the scientific method.

(U) The basic idea of _The Bible Code_ is that messages--presumably from God--are hidden within the Hebrew text of the Pentateuch, the five Books of Moses. These messages can be found by looking at "equidistant letter sequences" (ELSs) of the text with all spaces removed. An ELS is just a decimation of the message, to use some of our terminology. The first sentence of this review yields the ELS with a skip code of 4: LSYYCICR....

(U) By examining all possible ELS with a computer, strange and wonderful messages appear. The problem is that there's no way to know in advance how they will appear. Will they be written horizontally or vertically? Will critical words be sequential, or parallel, or intersecting in the array of letters? It's only after finding an important word or phrase that Drosnin recognizes its placement as significant. This is not good science.

(U) A significant problem for me is that Drosnin tacitly assumes he is working with THE true version of the Pentateuch. There are many ancient versions of the Pentateuch, some differing from each other in only minor spellings or variations. These differences do not affect the meaning of the text, but they destroy the ELS. A variant spelling of a word puts every ELS "off cut" after it.

(U) Another problem is that none of the mathematics is explained in the book, so readers cannot confirm Drosnin's use of someone else's math. Finally, I do not read Hebrew and was thus at Drosnin's mercy in explaining the significance of words.

(U) _The Bible Code_ was reviewed in "Notices of the AMS" (vol. 44, no. 8, Sept. 1997, pp. 935-939). Shlomo Sternberg was amazingly harsh on the four mathematicians who wrote Drosnin's introduction. Sternberg said in the Notices, "they have not only brought shame on themselves, but they have disgraced mathematics." Letters to the editor in the November and December issues continued the controversy.

(U) There is a WWW page set up to debunk "The Bible Code" (In Search of Mathematical Miracles, http://cs.anu.edu.au/~bdm/dilugim/index.html). The authors find equally striking ELS "messages" in _Moby Dick_ and _War and Peace_. There is also a letter denouncing the book signed by 19 prominent mathematicians, including Persi Diaconis.

(U) I enjoy reading science fiction and fantasy, but I prefer it clearly identified. Mr. Drosnin seems to have made a sincere attempt to apply some subtle statistical arguments to the problematical area of Biblical prophecy. For me, at least, he has used poor statistics to find

unconvincing prophecy.

.....

//

6. (U) COMMUNITY NEWS

6a. (~~FOUO~~) Cryptologic Mathematician Program (CMP) News
by [redacted]

(U) The Cryptologic Mathematician Program is pleased to announce the following:

Promotions:
[redacted]

Cryptologic Mathematician Professionalization Certificates were received by:
[redacted]

The following received Cash Awards:
[redacted]

The following received Awards from the Mathematics Education Partnership Program (MEPP):
[redacted]

[redacted] received a GWU Certificate in Telecommunications.

CONGRATULATIONS TO ALL!!

6b. (~~FOUO~~) Computer Communications Analysis Center Established
(Reprint of Announcement by [redacted] Chief Z6)

(~~C-CCO~~) To keep pace with the ever increasing SIGINT challenges posed by the diversity and pervasiveness of computer communications, Z6 has

(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

established the Z6 Computer Communications Analysis Center (CCAC), effective immediately. The CCAC is responsible for the successful execution of the signals analysis mission against computer communications. The Center represents a significant reallocation and repositioning of resources by Z6 to address this difficult problem. Upon final approval of the Center's Mission and Functions statement, the organizational designator of the Center will be Z607.

(b)(3)-P.L. 86-36

(FOUO) [redacted] is the Chief of the CCAC, and [redacted] is the Technical Director. The center members are [redacted]

(C-CCO) The computer communications analysis problem is clearly too big to be solved by any single organization. The CCAC is committed to working closely with other internal NSA and external organizations to share solutions and address new problems as they arise. Initially, the CCAC will focus on increasing the level of expertise in the signals analysis work force in the technology and analysis of computer communications, developing new and enhancing existing protocol, application, and network analysis tools, and developing the lab capability to support analysis of new computer communications software and hardware, both by Z6 and by other organizations that require this capability.

(C-CCO) Over the next several weeks, the CCAC will be reaching out to other organizations in an effort to discuss areas of mutual interest, and establish the partnerships that are critical to the successful solution of computer communications analysis problems. In the meantime, if you have questions about the Center, or would like more detailed information about its specific plans and current projects, please feel free to contact Anne, Tom, or any of the CCAC members.

6c. (U) Letter to All Z Technical Library Users

(U) The Z Technical Library on NDCS can now be accessed only through the Z Home Page. There is an icon called TECHLIB. Double click on the icon and you may access the Z library.

(U) If you have accessed the program through the Z Library Home Page in the past month, you can no longer access it on that page. You can continue to use the program the same way as you did before when you accessed it on the library home page.

(U) I will continue to receive your library requests.

(FOUO) Please contact me if you have any questions.

[redacted]
Z Technical Library

(b)(3)-P.L. 86-36

//

[redacted]

7. ~~(FOUO)~~ PROBLEMS AND PUZZLES
by [redacted] (b)(3)-P.L. 86-36

7a. (U) Winners of KRYPTOS Kristmas Kwiz:

~~(FOUO)~~ Congratulations go to [redacted]
who both received fantastic winning scores of 99!

~~(FOUO)~~ Other entries were received from (in no particular order):

[redacted]

(U) Solution:

1. a. Before Christ and Anno Domini
   b. French horn and cor anglais

2. a. TOO MANY COOKS SPOIL THE BROTH
   b. GOVERNMENT COMMUNICATIONS HEADQUARTERS
   c. KRYPTOS KRISTMAS KWIZ
   d. MERRY CHRISTMAS AND A HAPPY NEW YEAR

3. a. (4! - 3)/.1r - 2
   b. (2 + 3) x 41
   c. (4! - 2)/.1 + 3!
   d. 4!/.1 - 2**3!
   e. .2**(-3) + .1**(-sqrt 4)
      3! x 4! + .1r**(-2)
      4!/.1r + 3**2
      (4! + 3 - 2)/.1r
      (sqrt 4 + 3)/(.1 x .2r)
      [(4 + 1) x 3]**2
      (4! - 3/2)/.1
      (4! + 1) x 3**2

   3!! x .21r + 4!
   .2 x 3!! + .1**(-sqrt 4)
   (3!/.2r - sqrt 4)/.1r
   4!/.1 - 3/.2
   (sqrt 4 + 3)**2/.1r
   or (sqrt 4 + 3)/(.1r x .2)
   or [(4 + 1)/.3r]**2
   (23 + sqrt 4)/.1r

4. For each word ABCD, CDAB is also a word.

5. a. 3/4 consonants
   b. adjectives derived from Latin/not
   c. ID can be replaced by OR or OUR to form a noun/can't

6. GUERRE (C'EST MAGNIFIQUE, MAIS CE N'EST PAS LA with THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG). Both Q's were changed to O's.

7. ALL'S FAIR IN LOVE AND WAR.

8. ka (SAGA CITY) be (DISC LOSE) hc (PORT IONS)
   ld (STUD IOUS) fi (MODE RATE) jg (RAVE NOUS)

(b)(3)-P.L. 86-36

[redacted]

9. a. USER (HE-A-RD, TA-B-LE, FO-C-AL etc)
   b. CLUE (word scores - sums of values of letters, A=0 etc. - are 30, 31, 32)
   c. KILL (each word contains two consecutive letters of the alphabet; AB, BC, CD etc.)
   d. CLIFF (reversing the order of the words, the first and last letters spell (C)ENTIGRADE and (F)AHRENHEIT
   e. GUYANA (first letter of capitals is A, B, C....)
   f. ALGORITHM (words derived from Japanese, Icelandic, Hindustani, German..)
   g. VISITING (words contain, in order, I, II, III, IV, V....)
   h. PACK (preceding numbers - or the word "point" - give 3.1415926
   i. SHRINKING (associated colours form a rainbow)
   j. OVEREXCITABLE (characteristic, number of syllables)
   k. OVEREXCITABLE (characteristic, number of vowels)
   l. LARK (each bird starts with the second letter of the previous bird)
   m. WILFUL (first and last letters spell out WHORLOW and WARRELL)
   n. TASTE (first letter T, middle letters spell out KRYPTOS)
   o. ANSWER (first letter in reverse alphabetic order, middle letter(s) are points of the compass)
   p. SATIN (words include two letters for day of week and tonic solfa)
   q. AMBIDEXTROUS (half the word from the first half of the alphabet, the other half from the last, alternating, word lengths increase by 2)
   r. NAPE (the first one or two letters give the symbols for the elements in order of atomic number
   s. JOTTER (each word contains the appropriate letter in the alphabet followed by the name of a mammal - A GNU, B BAT, C ELAND etc.)
   t. GIRT/BUMF (last two letters are the first two slid by 1, 2, 3....)

10. a UPS AYU DUMB DOGS COW SOFTA POPS ASP
    ONE TWO FOUR FIVE SIX EIGHT NINE TEN

    b ECHE UGLI RICH FOCI COTE TOFU NENE SKEW PACA
    ALFA ECHO GOLF KILO LIMA MIKE PAPA XRAY ZULU

11. a. ABsConDEd, FiGHtIng, JacKaL, MoNOgraPh, QueeReST, UnderVieWer, oXYgeniZe. (7)
    b. ABaC, DEaF, GHI, JaK, LiMN, OP, Qua, ReST, UVa, WaXY, Zo. (36)

12. a. DRUB GIFT HEMP JACK LYNX VOWS
    b. JAZZ JACK VAMP VAST WELD VERB
    BEND BECK FIZZ WILD SPIV CHID
    BOWL GOWN FORK FROG THUG GULF
    JUNK JUMP HYMN NYTH CYST SPRY

13. a. 7 - 6 (each letter of KRYPTOS scores a goal)
    b. 3 - 2 (number of letters which contain a closed space - a, b, d, e, g, etc.)

14. Between EMPIRE and DOC.
    The list comprises words, each of which is associated with another word, and these other words are in alphabetical order. There are seven themes, with 8 members each:

    xAIL FAIL SAFE, HAIL STONE, JAIL BIRD, MAIL BOX, NAIL

(b)(3)-P.L. 86-36

9/24/2010

	BITING, RAIL WAY, SAIL OR, TAIL BACK
Bands	BEACH BOYS, HOT CHOCOLATE, BEE GEES, IRON MAIDEN, SEX PISTOLS, STATUS QUO, ROLLING STONES, DIRE STRAITS
NATO phonetics	CHARLIE BROWN, GOLF COURSE, HOTEL CALIFORNIA, INDIA RUBBER, KILO GRAM, PAPA DOC, SIERRA NEVADA, YANKEE DOODLE
Vegetables	BEAN BAG, CABBAGE WHITE, CAULIFLOWER EAR, MARROW BONE, MUSHROOM CLOUD, ONION RINGS, PEA SHOOTER, PEPPER MINT
Furniture	ARMCHAIR THEATRE, BED SIT, CABINET PUDDING, CHAIR LIFT, COUCH POTATO, OTTOMAN EMPIRE, STOOL PIGEON, TABLE FOOTBALL
US states	CALIFORNIA GIRLS, INDIANA JONES, KENTUCKY FRIED, MINNESOTA FATS, RHODE ISLAND RED, TENNESSEE WILLIAMS, VIRGINIA CREEPER, WASHINGTON IRVING
2B or not 2B	A SEA, AND ARROWS, BE THAT, QUESTION WHETHER, TAKE ARMS, THE MIND, TO SUFFER; leaving OUTRAGEOUS FORTUNE

15. a. CIRCLE SLICER CLEARS SAUCER SQUARE
    b. BLACK CHALK LATCH WATCH WITCH WHITE
    c. PURPLE RAPPEL PAROLE GALORE ORANGE OARING ORIGIN INDIGO

16. 17 BABOON BADGER BAT BEAR BEAVER BOAR DOG HARE HART HARTEBEEST HORSE RAT SHREW TARSIER TIGER VERVET WOMBAT

17. a. None is divisible by either of its digits
    b. Each is co-prime to both its digits

18.

Q	Z	H	V	J	
RAY	KIN	CUD	FEW	LOG	leaving S
T	P	M	X	B	

19. a. 3: BLAST
    LYNCH
    ANGRY
    SCRUM
    THYMY

    b. 14: TEENE
    EPEES
    EEVEN
    NEEZE
    ESNES

20. a. Chambers b. (Wilkie) Collins c. OED
    d. Webster e. Dictionary f. Samuel Johnson

21. All are spelt differently in the US and the UK

22. The number of months in which each letter appears

23. The number of letters in each number, when spelt out, also forms a magic square.

24. 474 (Good King Wenceslas, in the "key" of 4)

25. a. 5277 (digits sum to 21; others sum to 20)
    b. 3194 (perfect cube, backwards; rest perfect squares, backwards)
    c. 1512 (7 x perfect cube; rest are 7 x perfect square)
    d. 5760 (16x18x20; rest are product of three consecutive numbers)
    e. 4152 (spells BEAD backwards, A=1 etc; rest spell out words forwards)

(b)(3)-P.L. 86-36

9/24/2010

26. a. a. 281 (Sum of numbers in preceding matrix)
b. 9 (Number of digits in the matrix)
c. 217 (x^3 + 1)
d. 64 (difference of a. and c.)

b. 10 would also be true

27. TIP: TYPEWRITER, TOP ROW

28. 97

29. a. WISHING

b.
```
    S  O  C  I  E  T  Y
  K   A     B     C     D
  R     E     F     G
  Y   H    I/J    K     L
  P       M     N     O
  T   P     Q     R     S
  O       T     U     V
  S   W     X     Y     Z
```

7b.(U) February puzzle
(Taken with permission from the pages of the Grey Labyrinth at http://www.wx3.com/labyrinth/index.htm if you have an outside account.)

(U) The Counterfeit Coin

(U) Working at a reserve bank in beautiful Puzzlania, you are in charge of the destruction of counterfeit tender. Due to bad planning and a lack of originality bordering on plagiarism on behalf of the Puzzlanian treasury, the Puzzlanian dollar looks a lot like a U.S. penny, right down to the "UNITED STATES OF AMERICA - ONE CENT" on the back. In fact, the only difference between them is the grade of the copper. As a result, a Puzzlanian dollar doesn't weigh quite the same as an American penny.

(U) Well, you can probably guess what the number one source of counterfeit currency in Puzzlania is. So day after day, you have thousands of (Puzzlanian) dollars worth of U.S. pennies melted down to provide the raw materials for real Puzzlanian dollars.

(U) One day, on impulse, you pocket one of the counterfeits as a souvenir. While working with the analytical balance on a batch of real dollars, you accidentally mix the counterfeit coin with seven real coins near the end of your shift.

(U) It is imperative that you remove the fake from the real coins, or you'll lose your job (and go to prison!). Because the analytical balance uses very expensive electronic sensors, each employee has a limited number of "balancings" per shift.

(U) Each weighing on the balance will tell you which of the two samples is heavier, or if they are equal in weight. Puzzlanian dollars are identical in weight to within a microgram. American pennies, with their imperfections, are always heavier or lighter. Using the balance, you can compare any two piles of coins with each other; however, you have only the eight coins at your disposal.

(b)(3)-P.L. 86-36

(U) What is the fewest number of weighings which will tell you correctly which is the counterfeit coin?

(~~FOUO~~) Send all solutions, as well as puzzle submissions, to [redacted]

[redacted]

//

8. (U) LETTER TO THE EDITOR

(~~FOUO~~) "More about Looking at the Data"
by [redacted]

(b)(3)-P.L. 86-36

(U) Editor's note:

(~~FOUO~~) We received the following letter in response to "Some Things Never Change" by [redacted] in the January 1998 _Tales of the KRYPT_.

(U) Dear _Tales of the KRYPT_ Editor,

(~~C-CCO~~) [redacted] item on looking at the data reminded me of when I was working on manual cryptosystems. I always felt that an experienced person should handle the editing of the intercepted messages since the more experienced analyst who had a 'feel' for the traffic might be more likely to notice anomalies when they occurred.

(~~C-CCO~~) This idea proved true when an enciphered code book system stopped reading due to the code book changing simultaneous to the enciphering key pages changing. A message arrived that was just a mess. Later that message was resent and enciphered correctly. An intern in the office asked why we should bother keeping that trashy version of the message around when we had received a nice, clean copy of it later. I explained that that message might be THE one that gets us into the changed system. And it was. Comparing the poorly enciphered message with the good version of it showed what went wrong in the first version. And, knowing what went wrong showed how to do it right. But this message pair would not have been found if a person had not been looking at each and every message that arrived. Looking at the data is time-intensive work (that some people consider demeaning) but it is one of the most critical steps in cryptanalysis with benefits that pay off.

Thank you,
[redacted]

//

9.(U) EDITORIAL CORNER

(b)(3)-P.L. 86-36

REMINDER: (U) Submissions for the March issue are due by February 20. PLEASE NOTE: (U) All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION-MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the editorial board.

[redacted]

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

(b)(3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

~~TOP SECRET//COMINT~~

(b)(3)-P.L. 86-36

[redacted]

~~TOP SECRET//COMINT~~

~~(S)~~ *POC:* [redacted], *info*
(U) *Last Modified: 10/30/2002 11:42:23*
(U) PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
March 1998

//
****

++
//

(b)(3)-P.L. 86-36

(U) TABLE OF CONTENTS:

1. (U) Calendar of Events

2. (U) Cryptanalysis Career Panel (CACP) News:

2a. (U) Certifications, CACP Personnel Changes, PQE Registration

2b. (~~FOUO~~) 59th Professional Qualification Examination in Cryptanalysis by [redacted] Executive, Cryptanalysis Career Panel

2c. (U) New Definition for Cryptanalysis

3. (U) KRYPTOS Society News: Gift Certificate Winners for 1998 Membership Drive

4. (U) Technical Articles

(~~C-CCO~~) Z22 Technical Efforts: Cryptovariable Diagnosis

5. (U) Community News: Women in Mathematics (WIMS) at NSA

6. (~~FOUO~~) Community History: Remembering the Unsung Women Who Made Software History - PART I provided by [redacted]

7. (~~FOUO~~) Problems and Puzzles by [redacted]

7a. (U) Answer to February Puzzle

7b. (U) March Puzzle

8. (U) Letter to the Editor

(~~FOUO~~) Regarding [redacted] Evaluation of "The Bible Code" in the February Tales of the KRYPT_, by [redacted]

9. (U) Editorial Corner

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

//

1. (U) CALENDAR OF EVENTS

Mar 23-27	(U) CARD '98 at CSE
Mar 30-April 3	(U) CRYSCO at NSA
PLAN AHEAD	
Apr 10	(U) Deadline to register for CA PQE (See 2b.)
Apr 13-17	(U) CA-305 at NSA
May 5, 6	(U) CAPQE (See 2b.)
May 11-15	(U) ACE at GCHQ
Jun 4	(U) CMI Mathfest at R & E Symposium
Nov 2-6	(U) CONSCRYPT '98 at CSE

//

2. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

2a. (U) Certifications, CACP Personnel Changes, PQE Registration

(U) CA Certification

~~(FOUO)~~ Congratulations to [redacted], newly certified cryptanalyst!

(U) New CACP Membership

~~(FOUO)~~ The CACP welcomes the following:

[redacted] (b)(3)-P.L. 86-36
as CACP Executive

[redacted]
as Members of the CA Career Panel

[redacted]
as Members of the Computer Program Evaluation Board

(U) CA PQE Registration

(U) Registration is now open for the May 1998 Professional Qualification Exam. Sign up in the CACP office (OPS 2B 3036D).

2b. ~~(FOUO)~~ 59th Professional Qualification Examination in Cryptanalysis by [redacted] Executive, Cryptanalysis Career Panel

(b)(3)-P.L. 86-36

[redacted]

(U) The 59th Professional Qualification Examination in Cryptanalysis (CAPQE) will be given on Tuesday, 5 May and Wednesday, 6 May 1998. Registered eligible aspirants should report both days at the time and location listed below:

BUILDING	ROOM	REPORT TIME	EXAM BEGINS	EXAM ENDS
FANX II	TBD	0815	0830	1230

This is an open-book exam. Aspirants may bring texts, notes or calculators, but are responsible for securely transporting such material to FANX II.

(U) The format for the CAPQE is a two-day, four-hours-per-day written test with eight questions presented each day. There may be at least one narrative-style question offered each day. The aspirant's final score for the exam will be the total number of questions answered correctly over the two days. The passing score will be determined before the exam begins by an expert panel of cryptanalysts.

(b)(3)-P.L. 86-36

~~(FOUO)~~ Each aspirant must verify his/her eligibility for the CAPQE with the CA Career Panel office -- H111, OPS 2B room 3036D, [redacted] Aspirants who have previously taken the CAPQE are eligible for the May 1998 offering; new PQE aspirants must successfully complete the introductory training courses (CA-107, CA-123 and CA-110), one year of cryptanalytic experience, and two diversity assignments. For new PQE aspirants, H111 must receive a copy of their Diversity Validation Form by COB 10 April 1998. A signed Privacy Act Statement must be included with this document.

(U) Eligible aspirants who wish to take this exam must register in the panel office between 2 March and 10 April 1998.

(U) There will again be PQE review sessions held during the month of April, which will be scheduled during lunch hours so as not to interfere inordinately with office work time. Review packets, including a schedule of the review sessions, will be e-mailed to each registrant. It is strongly suggested that aspirants prepare for these sessions by working the questions from the previous examinations. Aspirants should come to the review sessions with specific questions or examples to share. Since some of the review sessions will be held in small conference rooms, only those people taking the exam will be allowed to attend.

2c. (U) New Definition for Cryptanalysis

(U) Over the years, the Cryptanalysis Career Panel (CACP) has consciously attempted to broaden its own, and the CA community's, thinking beyond the traditional outlook. We have questioned how CA and the development of cryptanalysts will be affected by "one team, one mission."

(U) At an offsite that the Panel had in October 1997, there was discussion of CA experiencing an identity crisis. People weren't sure exactly what constituted "cryptanalysis". Our career field has broadened to include several related areas. Therefore, it has become difficult to determine where CA ends and other disciplines begin.

(U) We have created a definition of CA for several reasons: to let

(b)(3)-P.L. 86-36

[redacted]

people outside the field (future cryppies looking to cross-train, perhaps?) know what we are all about, to create a sense of identity for the people who call themselves cryptanalysts by defining what makes us special and different from other types of analysts or technical people, and to help our subcommittees (Technical Paper Evaluation Board, Computer Program Evaluation Board, Technical Track Review Panel) get a handle on what is considered CA when evaluating a paper, program, or tech track application. We hope it will also provide new knowledge and ideas about cryptanalysis at the Agency and a perspective on where CA is headed.

~~(FOUO)~~ The CA Career Panel welcomes comments from the community on this issue. If you have any thoughts or suggestions you would like to express, send them to the CA Panel office at h111@nsa.

DEFINITION OF CRYPTANALYSIS AS OF 980209

~~(C)~~ Cryptanalysis is the analytic investigation of cryptosystems and the recovery of unknown information system parameters (such as cryptovariables, cryptographic algorithms, or signalling parameters recovered via bit-stream analysis) which can be used to render unintelligible data intelligible. For an activity to be considered cryptanalytic, it must include an analytic component addressed at the recovery of some unknown component of the system. The reformatting, display or other manipulation of cipher or of plain text with complex signalling parameters is not a cryptanalytic activity.

~~(FOUO)~~ The following set of examples is included to give CA certification committees, CA review panels, and CA Tech Track boards some sense of the issues to be considered in deciding if an activity is cryptanalytic and in evaluating diversity and experience requirements. This list should not be considered a complete taxonomy of all cryptanalytic activities, but rather a rough delineation of the CA domain. This list is meant to provide guidance in some of the areas in which the boundary between CA and not-CA is at issue. It should not be used as a checklist or substitute for careful evaluation of the case at hand. It remains a matter of subjective judgement whether or not an activity should be classed as cryptanalytic or not. In all the cases considered below, it is assumed that the level of analysis required is non-trivial. It is also assumed that the activity could be performed in support of either the SIGINT or INFOSEC mission; it is not the subject matter of the analysis that determines whether or not the activity is cryptanalytic, but the nature of the analytic process itself.

~~(C-CCO)~~ Cryptanalysis includes:

- Diagnosis of unknown cipher systems.
- Attack development to produce plaintext from cipher.
- Analysis and exploitation to produce plaintext from cipher.
- Analysis or evaluation of encryption algorithms.

(U) Certain jobs may or may not be cryptanalysis, but require cryptanalytic skills:

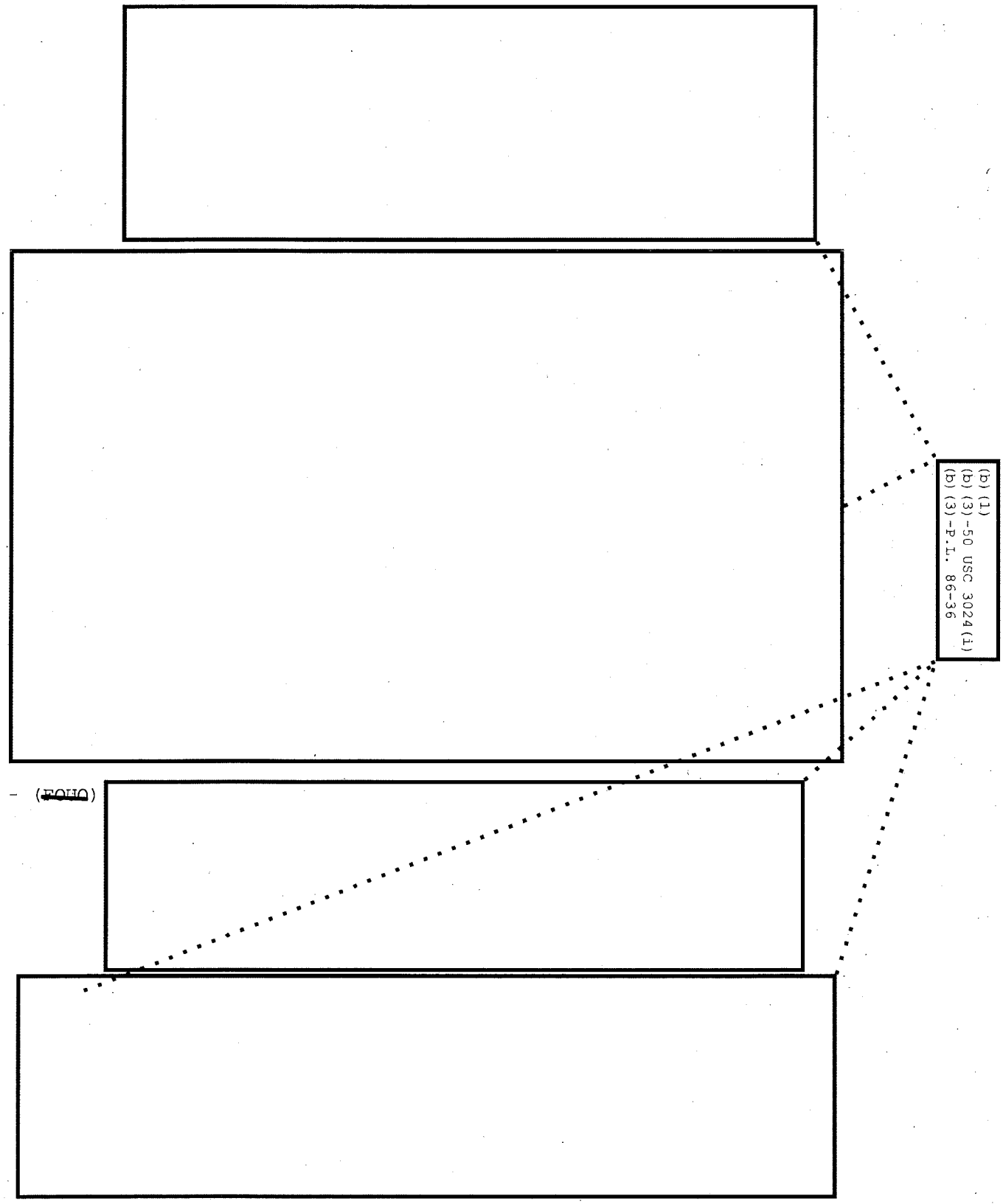
(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

- ~~(S-CCO)~~ Reverse Engineering of hardware or software

[redacted]

(b)(3)-P.L. 86-36

[redacted]



- (~~FOUO~~)

- (U) Analytic tool or technique development

IS cryptanalysis if it involves the development of a new analytic technique or the detailed understanding of an existing,

(b)(3)-P.L. 86-36

complex technique.

IS NOT cryptanalytic if the tool does not perform an analytic function even though it may be used in the analytic process.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(~~S~~) Cryptanalysis does not include:

- Data reformatting or editing.
- Development of data manipulation tools.
- Pure mathematical or language research.
- Processing of known protocols and communications systems.

(U) This definition will be placed on the CA Career Panel home page for future reference.

//

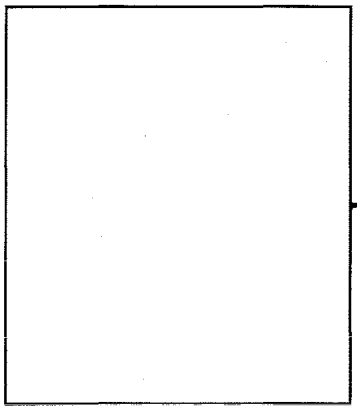
3. (U) KRYPTOS SOCIETY NEWS: Gift Certificate Winners for 1998 Membership Drive

(~~TOUO~~) Thanks to everyone who participated in the 1998 KRYPTOS membership drive! The lucky winners of Borders Gift Certificates are:

[redacted]

(b)(3)-P.L. 86-36

[redacted]



(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

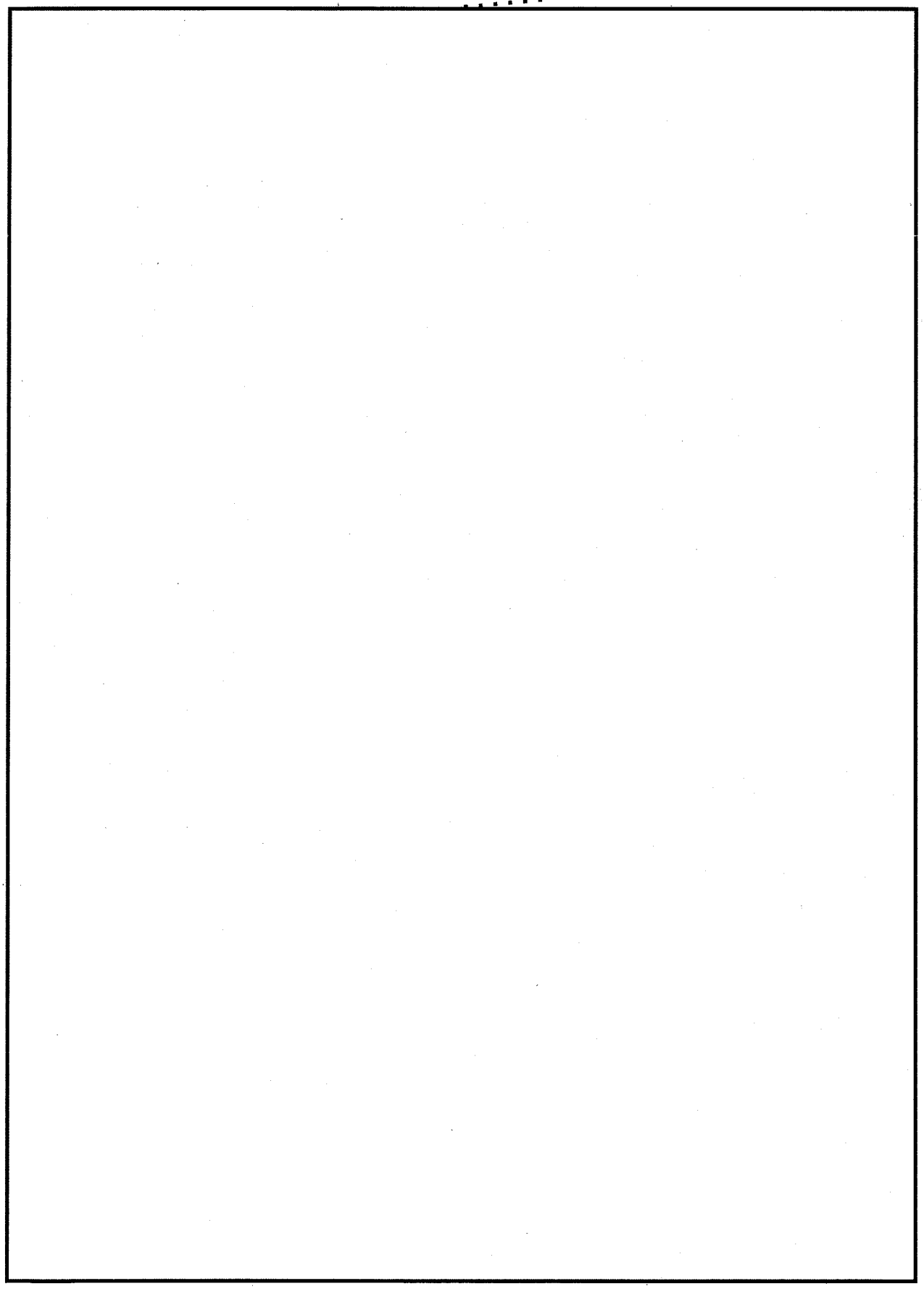
4. (U) TECHNICAL ARTICLES

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(C-CCO)~~ Z22 Technical Efforts:
(This is the first in a series of articles describing some of the cryptanalytic work performed in Z22 over the past year.)

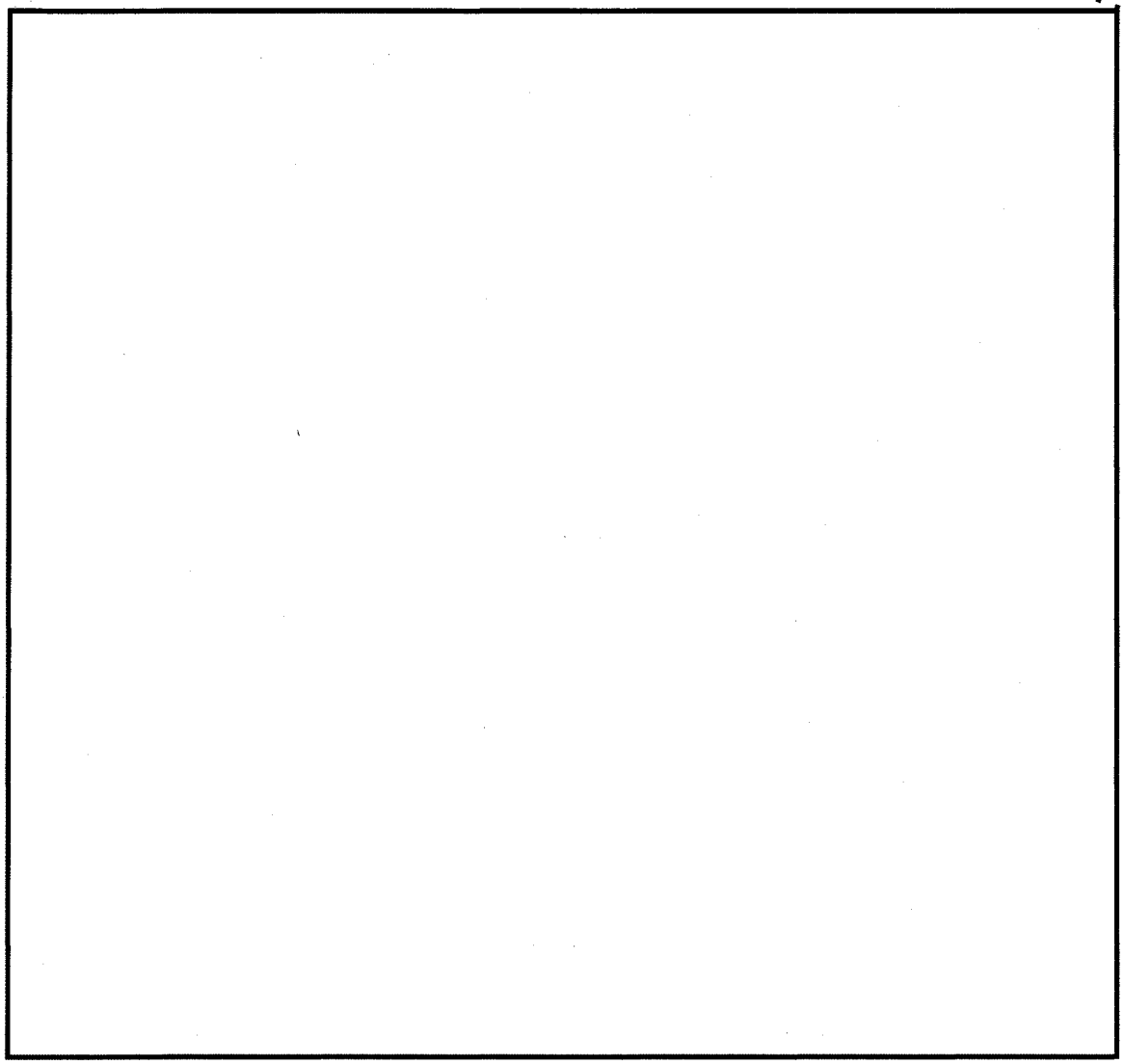
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



1. [redacted] "A Short Circuit of Random Number Generators", R51/TECH/004/93.
2. Knuth, "The Art of Computer Programming", Volume 2, Chapter 3, Random Numbers.

"""""""

~~(FOUO)~~ For more information on WIMS, please see our homepage at:

[redacted]

~~(FOUO)~~ If you would like to become a voting member of WIMS, please notify our president, [redacted] and she will include your name on the membership list.

(b)(3)-P.L. 86-36

//

6. ~~(FOUO)~~ COMMUNITY HISTORY: Remembering the Unsung Women Who Made Software History - PART I
provided by [redacted]

~~(FOUO)~~ (NOTE: This is the first of two articles provided by [redacted] in honor of Women's History Month (March). They came from two November 1996 issues of the _Wall Street Journal_ - "THE FRONT LINES" by Thomas Pitzinger, Jr.)

(U) Do you know the story of the first computer programmers--how they gave to history, how little history gave back to them, and what it means for the rest of us.

(U) In 1945, the clacking of adding machines and clouds of cigarette smoke filled a university-owned row house along Walnut Street in Philadelphia. Inside, dozens of women calculated trajectories to help wartime artillery gunners take aim. Men, the Army reasoned, lacked the patience for such tedium--a single problem might require months of work.

(U) The Army called the women "computers." One of them, Jean Bartik (nee Jennings), was a 20-year old math prodigy recruited from the farms of Missouri. Another, Betty (Snyder) Holberton, was the granddaughter of an astronomer who spent her childhood steeped in classical literature and language. The women formed a tight fellowship, drawn together by youth, brains and the war effort; Ms. Bartik alone had three brothers in the military.

(U) One day word spread that the brightest "computers" were needed to work a new machine called the Electronic Numerical Integrator and Computer, or ENIAC--a steel behemoth, 100 feet long and 10 feet high, built of 17,480 vacuum tubes in an engineering building at the University of Pennsylvania. Created by a visionary physicist named John Mauchly and a brilliant, mercurial graduate student named Presper Eckert, it was the first electronic computer, intended to automate the trajectory calculations the female computers performed by hand.

(U) Running the ENIAC required setting dozens of dials and plugging a ganglia of heavy black cables into the face of the machine, a different configuration for every problem.

(U) It was this job--"programming," they came to call it--to which just six of the young women were assigned: Marlyn (Westcoff) Meltzer, Ruth (Lichterman) Teitelbaum, Kay (McNulty) Antonelli and Frances (Bilas) Spence, as well as Ms. Bartik and Mrs. Holberton. They had no user's guide. There were no operating systems or computer languages. Just hardware and human logic. "The ENIAC," says Ms. Bartik, now 71, "was a son of a bitch to program."

(b)(3)-P.L. 86-36

[redacted]

(U) The first task was breaking down complex differential equations into the smallest possible steps. Each of these had to be routed to the proper bank of electronics and performed in sequence--not simply a linear progression but a parallel one, for the ENIAC, amazingly, could conduct many operations simultaneously. Every datum and instruction had to reach the correct location in time for the operation that depended on it, to within 1/5,000th of a second.

(U) Yet despite this complexity, the Army brass considered the programming to be so much clerical work; that it was women stringing the cables only reinforced this notion. Their government-job rating was SP, as in "subprofessional." Initially they were prohibited as security risks even from entering the ENIAC room, forcing them to learn the machine from wiring diagrams. When finally admitted, they sometimes had to straighten the clutter of gear the engineers left overnight.

(U) Finally, in February 1946, the scientists were ready for the ENIAC's official unveiling. A test problem involving the trajectory of a 155-millimeter shell was handed to Jean Bartik and Betty Holberton for programming. The machine executed flawlessly, calculating the trajectory in less time than it would take the bullet to land. After the demonstration, the men went out for a celebratory dinner. The programmers went home.

(U) In the 50 years since, their legacy is confined mainly to Movietone footage and sepia photos--women standing alongside the machine, as if modeling a Frigidaire. Why was history so ungenerous? Partly because in the awe surrounding the machine itself, the hardware was seen as the whole story (unlike today, when the action is in software). In addition, three of the programmers married engineers with top jobs on the ENIAC (Kay McNulty married co-inventor John Mauchly), making them wives first in the eyes of the history makers and history writers.

(U) A copious, definitive history of the ENIAC, written by the Army ordnance officer who commanded the project, merely lists the programmers names (misspelling one of them) and identifies which of the engineers they married.

(U) The greater injustice is not history's treatment of the women but its resistance to revision. As a Harvard undergraduate in 1984, Kathryn Kleiman felt like a misfit programmer until she encountered a footnote in a book remarking that programming had begun as a female field. Now a computer-law attorney with Fletcher, Heald & Hildreth in Rosslyn, VA, Ms. Kleiman has devoted years to producing a video documentary about the ENIAC programmers, five of whom are living.

(U) But software companies have turned a cold shoulder to Ms. Kleiman's fund-raising efforts, refusing to accept that the women could have contributed so much. Until Ms. Kleiman made an issue of it, most of the programmers had not even been invited to the gala dinner in Philadelphia in February 1996 celebrating the 50th anniversary of the ENIAC.

(U) Without the ENIAC women, "I absolutely think that computing and programming would be different today," Ms. Kleiman insists.

(U) [Part II will appear next month.]

(b)(3)-P.L. 86-36

"""""""

//

7. (FOUO) PROBLEMS AND PUZZLES (b)(3)-P.L. 86-36
by [redacted]

7a.(U) February puzzle
(Taken with permission from the pages of the Grey Labyrinth at http://www.wx3.com/labyrinth/index.htm if you have an outside account.)

(U) The Counterfeit Coin

(U) Working at a reserve bank in beautiful Puzzlania, you are in charge of the destruction of counterfeit tender. Due to bad planning and a lack of originality bordering on plagiarism on behalf of the Puzzlanian treasury, the Puzzlanian dollar looks a lot like a U.S. penny, right down to the "UNITED STATES OF AMERICA - ONE CENT" on the back. In fact, the only difference between them is the grade of the copper. As a result, a Puzzlanian dollar doesn't weigh quite the same as an American penny.

(U) Well, you can probably guess what the number one source of counterfeit currency in Puzzlania is. So day after day, you have thousands of (Puzzlanian) dollars worth of U.S. pennies melted down to provide the raw materials for real Puzzlanian dollars.

(U) One day, on impulse, you pocket one of the counterfeits as a souvenir. While working with the analytical balance on a batch of real dollars, you accidentally mix the counterfeit coin with seven real coins near the end of your shift.

(U) It is imperative that you remove the fake from the real coins, or you'll lose your job (and go to prison!). Because the analytical balance uses very expensive electronic sensors, each employee has a limited number of "balancings" per shift.

(U) Each weighing on the balance will tell you which of the two samples is heavier, or if they are equal in weight. Puzzlanian dollars are identical in weight to within a microgram. American pennies, with their imperfections, are always heavier or lighter. Using the balance, you can compare any two piles of coins with each other; however, you have only the eight coins at your disposal.

(U) What is the fewest number of weighings which will tell you correctly which is the counterfeit coin?

(U) Solution:

The fewest number of weighings is three. There are several paths to take. Here is only one possibility, given by Jennifer George: label the coins 1 through 8.
In the first weighing, weigh 1234 vs. 5678.
    If 1st light, 2nd weighing:125v346
        If 1st light, 3rd weighing:1v2
            If 1st light ->Coin1 is light
            If 2nd light ->Coin2 is light
            If even   ->Coin6 is heavy
        If 2nd light, 3rd weighing:3v4
            If 1st light ->Coin3 is light

(b)(3)-P.L. 86-36

[redacted]

```
            If 2nd light ->Coin4 is light
            If even      ->Coin5 is heavy
        If even, 3rd weighing:7v8
            If 1st light ->Coin8 is heavy
            If 2nd light ->Coin7 is heavy
    If 2nd light, 2nd weighing:561v782
        If 1st light, 3rd weighing:5v6
            If 1st light ->Coin5 is light
            If 2nd light ->Coin6 is light
            If even      ->Coin2 is heavy
        If 2nd light, 3rd weighing:7v8
            If 1st light ->Coin7 is light
            If 2nd light ->Coin8 is light
            If even      ->Coin1 is heavy
        If even, 3rd weighing:3v4
            If 1st light ->Coin4 is heavy
            If 2nd light ->Coin3 is heavy
```

~~(FOUO)~~ Solutions were received from [redacted]

[redacted]

7b. (~~FOUO~~) March puzzle (courtesy of [redacted]

(U) Jennifer and Dan are about to solve the 13-coin problem with three weighings when someone decides to throw in their two cents. Luckily Jennifer catches one of the new coins in midair, and the interloper assures everyone that both new coins are genuine. How can the lone counterfeit coin be found in the pile of 14 coins with just three weighings? (This is an extension of the previous puzzle - you are still to assume that all the good coins weigh the same, and the counterfeit coin has a different weight, but you don't know if it is heavier or lighter.)

~~(FOUO)~~ Send all solutions, as well as puzzle submissions, to [redacted]

[redacted]

(b)(3)-P.L. 86-36

//

8. (U) LETTER TO THE EDITOR

(~~FOUO~~) Regarding [redacted] Evaluation of "The Bible Code" in the February _Tales of the KRYPT_, by [redacted]

(U) Editor's note:

(~~FOUO~~) We received the following letter in response to "An Evaluation of 'The Bible Code,' (the actual code described in the book of the same name), by [redacted] CMP Program Director, in the February 1998 _Tales of the KRYPT_.

(U) Dear _Tales of the KRYPT_ Editor,

(U) [redacted] is bang-on in describing this as pseudo-scientific and portraying a general (I'd say, "complete") misunderstanding of the scientific method.

(b)(3)-P.L. 86-36

[redacted]

(U) I had to deal with correspondence from some of these seriously misguided individuals during my year at the [redacted]. I later mentioned one of these cases to Woody Dudley (Editor of the MAA's "College Math Journal" and author of _Numerology, or What Pythagoras Wrought_), saying that I had initially believed one should treat such people gently. However, doing so only generates ten times the heat for the second iteration. Xerox must be making a killing on the business of these people alone. Woody and I are now in complete agreement that such individuals must not be mollycoddled, but must be told point-blank that they are wrong; that they misunderstand the scientific method; that they misunderstand the concept of proof; that they would be much better off to drop consideration of the matter entirely; and that you (i.e., I) will not reply to any further correspondence. There can be no middle ground related to such horsefeathers. [redacted] (b)(6)

(U) To see where such thinking leads, read Woody's book, or either of his previous two: _Mathematical Cranks_ and _The Trisectors_.

~~(FOUO)~~ Cheers,

[redacted]

"""""""

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

(b)(3)-P.L. 86-36

[redacted]

(U) POC: [redacted] *info*
(U) *Last Modified: 10/30/2002 11:42:22*
(U) PE EXTERNAL PAGE

(b)(3)-P.L. 86-36

****
* TALES OF THE KRYPT *
****
April 1998

//
****

++
//

(U) TABLE OF CONTENTS:

1. ~~(TOUO)~~ Perspective: by [redacted] Chief, [redacted] assigned to the DDT

2. (U) Calendar of Events

3. (U) Cryptanalysis Career Panel (CACP) News

3a. (U) New CACP Executive and Assistant Executive Announced

3b. (U) Non-monetary Awards for Service to the Cryptanalysis Technical Track

3c. ~~(TOUO)~~ CA Technical Track Criteria Changes

4. (U) KRYPTOS Society News: International KRYPTOS CA PQE Contest

5. (U) Technical Articles

5a. ~~(TOUO)~~ Matt on Math: "Two Famous Sums" by [redacted] CMP Intern

5b. ~~(TOUO)~~ "The Year 2000 is a Problem for Our Targets Too" by [redacted]

5c. ~~(TSC)~~ [redacted] by [redacted]

6. (U) Community News

6a. ~~(TOUO)~~ DO Skill Field Corner by [redacted], DO Skill Field Director for Cryptanalysis

6b. ~~(TOUO)~~ History: "Female Pioneers in the Computer Industry" - PART II of a 2-part series in honor of Women's History Month (March) provided by [redacted] Chief, Z609

7. ~~(TOUO)~~ Puzzles by [redacted]

7a. (U) Answer to March Puzzle

7b. (U) April Puzzle

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

8. (U) Editorial Corner

(b)(3)-P.L. 86-36

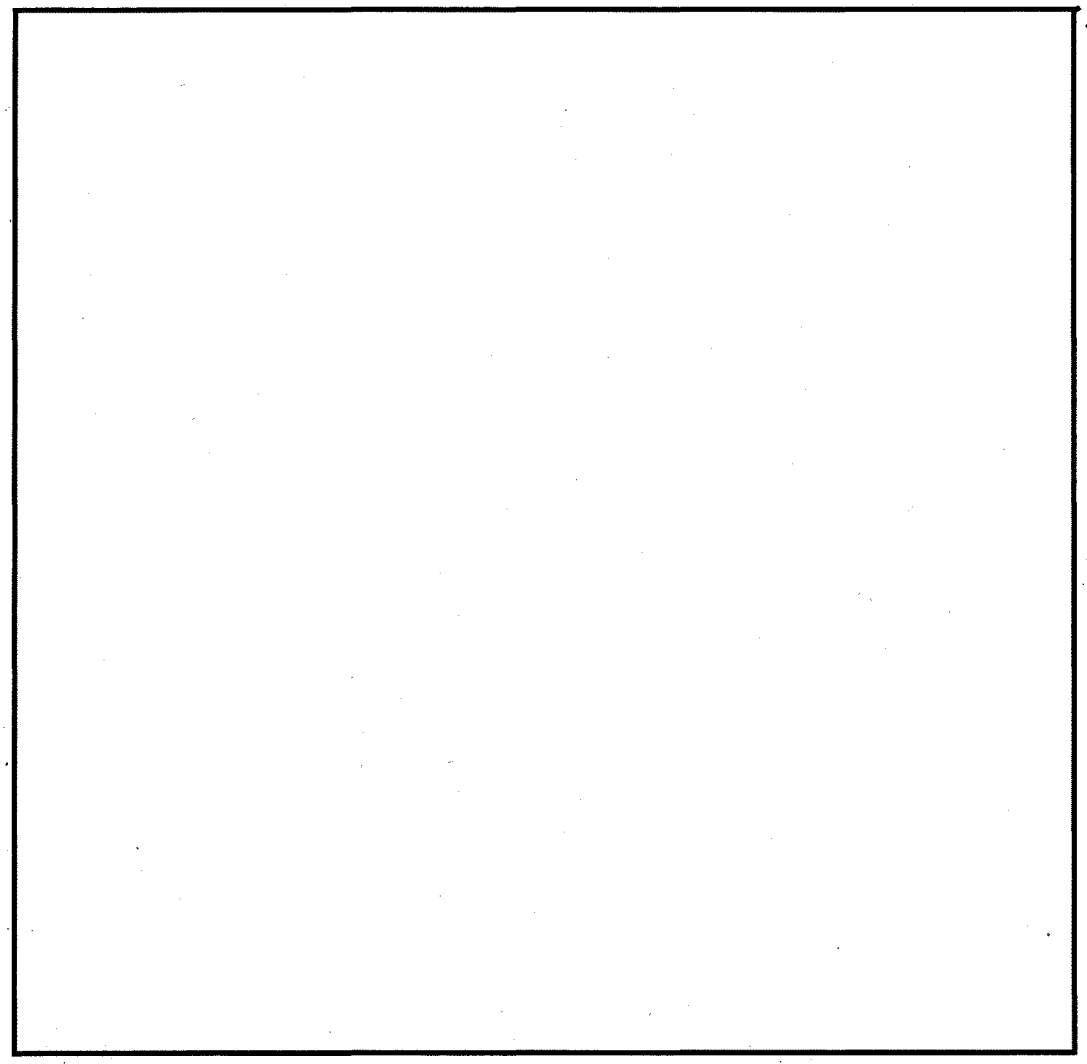
1. (~~FOUO~~) Each month this newsletter features the perspective of a Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of [redacted], now Chief, [redacted] assigned to the DDT, formerly Chief, [redacted] and prior to that Chief, Z2.

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(FOUO)~~ I've always enjoyed the SIGINT mission and had previously stepped outside the cryptanalytic community for brief periods. But now for a significant period of time, I've had the opportunity to lead a major activity which engages in its every aspect. It's exciting but intimidating; it's sometimes discouragingly hard but very often wonderfully rewarding; it's routine in some ways but unique in ways previously unimaginable to me. The people I've met and the places I've been have added a new and exciting dimension to my career. I challenge each of you to consider stepping outside the cryptanalytic community in order to return better prepared for carrying on your very important and still unique task of breaking the world's cipher systems.

****
//////////

2. (U) CALENDAR OF EVENTS

Apr 10	(U) Deadline to register for CA PQE
Apr 13-17	(U) CA-305 at NSA
Apr 13-17	(U) Z RSOC CA/SA Conference at NSA
Apr 20-24	(U) Signals and Analysis Development Conference at NSA

(b)(3)-P.L. 86-36

PLAN AHEAD

May 5, 6	(U) CAPQE
May 11-15	(U) ACE at GCHQ
Jun 4	(U) CMI Mathfest at R & E Symposium Center
Jun 22 - Aug 28	(U) SCAMP at LaJolla
Sep 11	(U) CMP Graduation, Friedman Auditorium, 1300
Nov 2-6	(U) CONSCRYPT '98 at CSE

"""
//

3. (U) CRYPTANALYSIS CAREER PANEL (CACP) NEWS

3a. (U) New CACP Executive and Assistant Executive Announced

(FOUO) The Cryptanalysis Career Panel is pleased to announce that [redacted] is on board as the new CACP Executive, replacing [redacted] Also, on April 25, [redacted] will take over for [redacted] as Assistant Executive. The panel is grateful to [redacted] for their outstanding service to Cryptanalysis for the past few years and is fortunate to have such capable replacements stepping into these pivotal positions. [redacted] may be reached on [redacted] for Professionalization, Technical Track and general career development guidance.

(b)(3)-P.L. 86-36

3b. (U) Non-monetary Awards for Service to the Cryptanalysis Technical Track

(FOUO) The following people were recently recognized with non-monetary awards for their service to the Cryptanalysis Technical Track.

With clock towers denoting at least two years of service on the CA TTRP or DO THAB:

[redacted]

With portfolios denoting at least one year of service:

[redacted]

(U) The CA Career Panel greatly appreciates the contributions that these individuals have made to furthering the technical health of the career field.

(b)(3)-P.L. 86-36

[redacted]

3c. (U) CA Technical Track Criteria Changes

(U) A subcommittee of the Senior Technical Track Board (STTB) has been tasked with studying and levelling all the skill fields' tech track criteria. There will be some changes to the CA tech track criteria as a result. The subcommittee is recommending that the new criteria be put into effect on 1 May, with all tech track applications received after that date being evaluated under the new criteria. This proposal and the individual skill fields' criteria have not yet been approved by the STTB, so the actual implementation date is still tentative. Watch this space and ESS topics 1284 (Cryptanalysis Career Panel) and 1263 (Technical Track) for more details.

"""""""

Then, adding the two together term-by-term we see that

2S = 101 + 101 + 101 + 101 + ... + 101

or

2S = 100 * 101

i.e. S = 10100/2 = 5050. This suggests a closed form for the sum of the first N integers: S = N*(N+1) / 2. Observe that when N is large, S is very large. In fact, as N approaches infinity, S grows without bound. We say that the infinite Gauss sum or "series" diverges.

(U) Another famous sum is called the "geometric series." The series

S = 1 + r + r^2 + r^3 + ... + r^k + ...

is called the geometric series with common ratio r. This is a series with an infinite number of terms. Let's see how a finite piece of S, say the first N terms, sums up. The "Nth partial sum"

S_N = 1 + r + r^2 + r^3 + ... + r^N.

Multiply S_N by the common ratio r:

rS_N = r + r^2 + r^3 + ... + r^N + r^(N+1).

Notice how the terms line up. Now, subtract rS_N from S_N:

(S_N - rS_N) = 1 - r^(N+1)

because all of the intermediate terms cancel out. Finally, we factor out S_N and divide to obtain a closed form expression for S_N

S_N(1 - r) = 1 - r^(N+1) or S_N = [1 - r^(N+1)] / (1 - r).

(U) This expression for S_N is perfectly valid provided N is a positive integer and r is NOT equal to 1 (because we can't divide by zero). What happens, however, if we let N approach infinity or grow without bound?

(U) Let's experiment with a C program and the geometic series with r = 0.5. To compile this program on your Sun computer, save the code to a file called (say) series.c then type gcc -o series series.c and run it with the call (say) series 1000 (or any positive integer 2 or larger) to compute the geometric series with 1000 terms. Feel free to change R_VAL and play!

```
#include
#define R_VAL 0.5

main(int ac, char **av)
{
  register int i;
  double r = R_VAL;
  double S;
  int N;

  N=atoi(av[1]);
  S=1.0+r; /* the first 2 terms */

  if(N==2) { printf("S=%f\n",S); exit(1); }
```

(b)(3)-P.L. 86-36

```
  for(i=2;i<=N;i++) { r*=R_VAL; S+=r; }

   printf("S=%f\n",S); exit(1);
}
```

(U) Here is the output for various input values:

N	series N
2	1.500000
10	1.999023
15	1.999969
16	1.999985
20	1.999999
21	2.000000
100	2.000000
1000000	2.000000

(U) Looks like S converged to the value 2 (up to the precision of my computer). In fact the series will converge to 2 as N approaches infinity. Why?

(U) Recall, that S_N = (1-r^(N+1))/(1-r). The only term in that equation involving N is r^(N+1). In this example, r=1/2. For large values of N, (1/2)^N is small and as N approaches infinity, (1/2)^N approaches zero. Hence, as N approaches infinity, S_N converges to 1/(1-r) which equals 2 when r=(1/2). The same argument applies for negative values of r. If r=(-1/2) then S converges to 1/1+(1/2) = 2/3. The argument breaks down (and the series diverges) when r^(N+1) becomes unbounded as N approaches infinity. This happens when |r| > 1. The final case to investigate is the case of r=(-1). Here the Nth term of the geometric series equals 1 or 0 depending on the parity of N, hence the geometric series diverges in this case [because the sequence of partial sums oscillates].

(U) Summarizing our results, we conclude that the geometric series

$$S = 1 + r + r^2 + r^3 + \ldots$$

converges to 1/(1-r) for -1 < r < 1 and diverges for |r| >= 1.

5b. (~~FOUO~~) "The Year 2000 is a Problem for Our Targets Too"
by [redacted], GCHQ Year 2000 Event Coordinator

(b)(3)-P.L. 86-36

(U) [N.B.: British spelling and usage have been preserved throughout this article.]

(~~S~~) The Year 2000 computer 'bug', when computers worldwide face possible failure as their internal clocks go from 99 to 00, could cause major problems worldwide. The total cost has been estimated to be anything up to $3.6 Trillion worldwide, and that is just for fixing or replacing systems. The legal bills afterwards are thought to be as much again. The effects are seen in considerably more than desk-top computers. In fact only 1% of microprocessor chips are thought to be in desk top computers at all. The rest are in equipment ranging from high tech weapons systems to domestic appliances like microwaves. Weapons command and control systems, nuclear reactors and air traffic control systems could all break down, with potential for loss of life. Power supplies are also at risk, since failure of embedded chips in oil rig pumping systems (BP are currently working against the clock to replace theirs) and even minor infrastructure breakdown could

(b)(3)-P.L. 86-36

[redacted]

jeopardise supplies of fuel to power stations, resulting in power cuts, and further equipment failures. Some estimate that Britain and the US will be reduced to 50% of their current power levels over January 2000. There is also great potential for financial fraud and computer hacking. These problems will affect the whole world: even the most advanced countries haven't the time or the resources to fix more than their most critical systems, and Europe is having to divert resources away from Year 2000 programming to cope with monetary union conversion. The countries which will be most heavily hit are, however, Russia and former Soviet countries, Eastern Europe, Turkey and China. These are heavily reliant on imported IT, and do not have the resources or the time to fix their problems. Given the worldwide scope of the problem, and the fact

[redacted] (b)(3)-P.L. 86-36

[redacted] In some cases intelligence will be the only source of information about Year 2000 remediation work--so it is worth looking for.

5c. [redacted] (b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

by [redacted]

[redacted]

"""""""

6. (U) COMMUNITY NEWS:

6a. (~~FOUO~~) DO Skill Field Corner
by [redacted] (b)(3)-P.L. 86-36

(U) Greetings! I'd like to take this opportunity to introduce myself in my new position as DO Skill Field Director for Cryptanalysis.

(U) The Skill Field Directors are newly created, full-time positions for each of the eight DO tech track skill fields. We will be working along with the career panels on technical health issues, and through the DO THAB to implement the Technical Track Program.

(~~FOUO~~) I sit in [redacted] and can be reached at [redacted] secure. My web page [redacted] will contain information about technical health issues affecting cryptanalysts, as well as information on Z Group Hiring and Language issues (my other two hats). The page is pretty sparse right now, but expect to see more there in the future.

(U) I will keep the CA community informed of initiatives in these areas and I welcome anyone to contact me with questions, suggestions, and concerns.

(~~FOUO~~) [redacted]

6b. (~~FOUO~~) History: "Female Pioneers in the Computer Industry" -
PART II of a 2-part series in honor of Women's History Month (March)
provided by [redacted]

(~~FOUO~~) (NOTE: This is the second of two articles provided by [redacted] in honor of Women's History Month (March). They came from two November 1996 issues of the Wall Street Journal - "THE FRONT LINES" by Thomas Pitzinger, Jr.) (b)(3)-P.L. 86-36

(U) Growing up near Philadelphia, Betty Holberton was left-handed, cross-eyed and mercilessly teased by her classmates. Her orchestra leader chided her for standing on the wrong side of the double bass. On her first day at the University of Pennsylvania, her math professor said she should be home raising children.

(U) Jean Bartik never quite fit in, either. Growing up in the farm fields of Missouri, she could outpitch her brothers in softball. She studied Latin as a hobby. In college she took physics and trigonometry, usually the only girl in class. Quirky and tenacious--the perfect attributes for becoming history's first computer programmers. Was their gender also a factor?

(U) The two of them, joined by four other young women, programmed history's first general purpose digital computer, the ENIAC. But Ms. Holberton and Ms. Bartik did not stop there. Their continuing work--spanning nearly 40 years, in Ms. Holberton's case--helped to create the computer industry as we know it today.

(U) They believed computers would flourish only if easy to program and operate. No matter how complicated computers are today, there is no doubt that they would be even less accessible if not for the work of these pioneers. "I spent half the day trying to figure out what people needed in a computer," Ms. Holberton says, "and the rest of the day trying to convince an engineer it was his idea."

(b)(3)-P.L. 86-36

[redacted]

(U) Following the Army's unveiling of the ENIAC in 1946, Jean Bartik joined a mathematician named Adele Goldstine in leading a team to revamp the machine as a "stored program" computer. This relieved programmers of the need to configure a new labyrinth of heavy cables for every equation the machine solved. The invention of internal programming is often attributed to the great mathematician John von Neumann, who published a paper on the breakthrough. Ms. Bartik and her team consulted regularly with Dr. von Newmann, but it was she who wrote the code.

(U) A short time later, in 1948, she and Ms. Holberton were reunited at a company called Eckert-Mauchly Computer Corporation, established by the two principal creators of the ENIAC. Eckert-Mauchly was creating a new machine called the Universal Automatic computer, or Univac--the first general purpose commerical computer, the device that would compile the 1950 census, predict Eisenhower's victory over Stevenson and ultimately revolutionize business.

(U) While the engineers were absorbed in technical blandishments, Ms. Holberton brooded over "human engineering," her way of saying the machine could be user-friendly. She created an instruction code called C-10, enabling programmers to control the computer with typewritten commands instead of dials and switches. She built the language around mnemonic characters--"a" for add, "b" for "bring," introducing an intuitive aspect to the hypertechnical practice of programming.

(U) The very look of the Univac embodied her thinking. In designing the control panel she put the numeric keypad alongside the keyboard so letters and numbers could be entered with equal ease. She insisted the intimidating black exteriors be abandoned, thus locking in gray as the color of choice for computing.

(U) But to what use would the Univac be put? Ms. Holberton headed the development of a "sort generator," a program organizing payroll, inventory and other data according to the unique parameters of the user. It was probably the first use of a computer to program its own application.

(U) Eckert-Mauchly was sold in 1950 to Remington Rand, which evolved into Speery Univac and ultimately into the Unisys of today. When M.I.T. Press brought out a history of the history-making machine in 1987, it was titled "A Few Good Men from Univac."

(U) Ms. Holberton remained in the thick of computing--though never in the spotlight--until 1983, first with the Navy and later the National Bureau of Standards. She knew the machines had to talk the same language if computing was to spread, so she led a committee to establish standards for the Common Business Oriented Language, or COBOL; it remains among the most widely used computer languages on Earth. She later played a similar role in the development of Fortran.

(U) Today, at 79, Ms. Holberton is partly paralyzed from a stroke but speeds around her nursing home in Rockville, MD in a wheelchair. The one visible momento of her trailblazing years is the steel nameplate, hanging on her wall, from Univac serial number 006. Ms. Bartik, 71, supports herself selling real estate in New Jersey.

(U) Programming started out as an exclusively female field. But as software began catching up to hardware in importance, men moved in and quickly moved ahead for good. Wherein may lie the deepest significance of the story.

(U) The programming challenges of the future are too huge to permit the discouragement of half the population. Yet the proportion of women

(b)(3)-P.L. 86-36

studying computer science has been declining for a decade. One reason may be the historical dearth of role models in significant positions. "Girls have an image of computer science being for boys," says Denise Gurer, an artificial-intelligence researcher at SRI International.

(U) As for her own pioneering role, Ms. Holberton remains modest. "Somebody would have done it if I hadn't done it," she insists. Maybe so, but would someone else have done it quite the same way?

"""""""

B. We have a set X of (3^n+1)/2 coins and a set Y of (3^n-1)/2 coins. One of these 3^n coins is wrong: if it's in X, it is light; if it's in Y, then it's heavy. We also have 2 correct coins. After weighing, we can identify the bad coin and say whether it is heavy or light. (Clearly the case of X heavy, Y light is also fine!)

(U) We prove these by induction.

If n=1, then A states that we have a good coin and a bad coin, we know which is which and we can identify whether the bad coin is heavy or light with 1 weighing. This is clearly true!

If n=1, then B states that X has 2 coins and Y has 1 coin, and one of the 3 is bad. We balance the 2 X coins. If they balance, the Y coin is heavy. If they don't, the lighter of the X's is the wrong coin.

We now assume that the above holds for n = N.

Consider case A for n = N+1. We have (3^(N+1)-1)/2 coins, one of which is wrong, plus 1 good coin.

We balance (3^N+1)/2 against (3^N-1)/2 plus the good coin.

If they balance, then one of the remaining (3^N-1)/2 is bad. But by assumption, we know we can solve this in N weighings.

If they don't balance, we can assume wlog that the (3^N+1)/2 are lighter than the (3^N-1)/2 + good.

Now balance (3^(N-1)+1)/2 "lights" and (3^(N-1)+1)/2 "heavies" against (3^(N-1)-1)/2 lights and (3^(N-1)-1)/2 heavies and 2 goods. If they balance, then the remainder, which consists of (3^(N-1)+1)/2 lights and (3^(N-1)-1)/2 heavies can be solved with (N-1) weighings by assumption. If they don't balance then, in either case, we have (3^(N-1)+1)/2 of one type and (3^(N-1)-1)/2 of the other (and at least 2 good coins) which we can solve in (N-1) weighings by assumption. In either case, we can solve case A for n = N+1 in (N+1) weighings.

Now consider case B for n = N+1. X contains (3^(N+1)+1)/2 lights and Y contains (3^(N+1)-1)/2 heavies. As above, balance (3^N+1)/2 lights and (3^N+1)/2 heavies against (3^N-1)/2 lights and (3^N-1)/2 heavies and 2 goods.

If they balance, then what remains is (3^N+1)/2 lights and (3^N-1)/2 heavies, which we can solve in N weighings by assumption.

If they don't balance, then either way, we have (3^N+1)/2 of one type versus (3^N-1)/2 of another (and at least 2 goods), which we can solve in N weighings by assumption.

Hence we can solve case B for n = N+1 in N+1 weighings.

We are, of course, interested in case A. Jennifer & Dan suggested the case N=3 (13 dubious and 1 good). We now see that, with 4 weighings, we can solve 40 dubious + 1 good. With 5, we can solve 121 dubious + 1 good etc.

The same reasoning as before shows that we cannot solve the case of (3^(N+1)-1)/2 "doubly dubious" (correct/light/heavy) plus 1 "singly dubious" (correct/light) so the above are, in some sense, optimal.

And now for the pretty stuff....

(b)(3)-P.L. 86-36

9/24/2010

Previously, I showed that, with 3 weighings we could not (fully) solve the case of 13 good/light/heavy ("doubly dubious") and 1 good/light ("singly dubious").

However, if we have access to 9 good coins (which we can assume since we're in a bank), then we can achieve the above, and in a pretty way that obviously generalises to more weighings.

Label the 13 doubly dubious coins 0 to 12 and the singly dubious coin 13.

We also label the light/heavy events:

Event 0 is when coin 0 is light
Event 1 is when coin 1 is light
...
Event 11 is when coin 11 is light
Event 12 is when coin 12 is light

Event 13 is when coin 13 is bad, i.e. light

Event 14 is when coin 12 is heavy
Event 15 is when coin 11 is heavy

...
Event 25 is when coin 1 is heavy
Event 26 is when coin 0 is heavy

All we have to do is express the label of each coin in base 3. Then at the t'th weighing, use the t'th digit to decide which side of the scales to put the coin. 0 = left, 2 = right, 1 = don't use this time.

So coin 0 always gets put on the left. Since 7 = 021 in base 3, we put coin 7 on the left for the first weighing, on the right for the second and don't use it for the third.

If the number of coins on left and right aren't equal, we use good coins to make up the difference.

At each weighing, if the left side is lighter, we assign a 0, if it's heavier, we assign a 2 and if both sides balance, we assign a 1. Concatenating these gives the label of the required event.

So, if we found Left Heavy then Left Light then Balanced, we would assign 201 (or 19 decimal) and deduce that coin 7 is heavy. The method has to work, since each coin follows a different weighing strategy and the event number just "follows" the bad coin.

This method clearly generalises to any number of weighings. With n weighings, we can solve the case with (3^n-1)/2 doubly dubious coins and 1 singly dubious coin. We will need 3^(n-1) good coins, since there are this many dubious coins, all on the left side, for the first weighing.

We can also solve the case with 3^n singly dubious coins, by labelling the coins 0 to 3^n-1 and letting event i mean that coin i is bad.

Without too much strain, we can also handle the intermediate case with D doubly dubious coins and (3^n-2D) singly dubious coins.

The method even generalises to other types of weighing apparatus, where there are N types of outcome, one of which is "balanced".

7b. ~~(FOUO)~~ April puzzle - Phonetic Phillers

(b)(3)-P.L. 86-36

This puzzle is taken with permission from the web page of Mike Pieja, http://members.aol.com/stannum/puzzle/main.htm if you have an outside account.
Credit for the puzzle goes to [redacted]

(U) Surely you've all seen puzzles such as this unimaginative specimen:

[ICE]_____[PUFF]

where the object is to insert one letter into each blank to make a word, and also makes a word or phrase when you combine these new letters with both the preceding "ICE" and the following "PUFF". In this case the answer is "CREAM", forming "ICE CREAM" and "CREAM PUFF". On this page, of course, there is no such mediocrity as that... Instead, try this extended filler chain, where each blank in a series must make a word or phrase, when paired with the letters in brackets on either side.

[TOU]___[TER]___[COR]___[TER]___[FALL]___[SIDE]

(TOUO) Send all solutions, as well as puzzle submissions, to [redacted]

[redacted]

(b)(3)-P.L. 86-36

"""""""

(b) (3)-P.L. 86-36

9/24/2010

~~TOP SECRET//COMINT~~

~~(C)~~ POC: [redacted] *info*
(U) *Last Modified: 10/30/2002 11:42:24*
(U) PE EXTERNAL PAGE

(b)(3)-P.L. 86-36

```
**********************************
*        TALES OF THE KRYPT      *
**********************************
```

May 1998

//
****

++
//

(U) TABLE OF CONTENTS:

1. ~~(FOUO)~~ Perspective: by [redacted], D/Chief, Z2.

2. (U) Calendar of Events

3. (U) KRYPTOS Society News:

   3a. (U) CMI/KRYPTOS Society Night at the Bowie Baysox

   3b. (U) Call for Suggestions for KRYPTOS Distinguished Members

4. (U) Community News

   4a. ~~(C CCO)~~ Call for Abstracts for NSA's Computer Communications Working Group (CCWG): C2C Target Development

   4b. ~~(FOUO)~~ History: "Women in Cryptology" -- Speech presented by Miss Ann Caracristi, Former D/DIRNSA, at NSA on 6 April, 1998 in commemoration of Women's History Month

5. ~~(FOUO)~~ Puzzles by [redacted]

   5a. (U) Answer to April Puzzle

   5b. (U) May Puzzle

6. (U) Editorial Corner

(b)(3)-P.L. 86-36

****
//

1. ~~(FOUO)~~ PERSPECTIVE - Each month this newsletter features the perspective of a Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of [redacted], D/Chief, Z2.

~~(TS CCO)~~ The air is full of talk of change, as usual. In thinking about what to write for this article, I remembered a debate I overheard while I was finishing up my final CMP tour in 1982. The discussion was about the expected impact of microprocessors on the business of

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

breaking codes. One side was pretty pessimistic, thinking the new flexibility and reduced costs would lead to such rapid changes in cryptoalgorithms we'd never be able to keep up. (Of course the pessimism was further fueled by concerns over DES, where it was just a matter of time until the spread of that algorithm would shut us down almost single-handedly!) The other side was more optimistic. I don't really remember their counterarguments - or even if they made explicit counterarguments - but I remember their confidence, their belief that we'd find a way to succeed, one way or another.

(U) Since that day, I, along with hundreds of others, have spent a lot of time and energy proving the optimists correct. In fact, I don't think the most optimistic person in the bunch would have predicted the quantitative or qualitative success we've enjoyed over the past 16 years. So maybe there's a lesson in all of this. Maybe when we face the unknowable future, the uncertainty of tomorrow, sure only that things will not be as they were, we have a choice to make, perhaps a psychological choice, between optimism and pessimism.

(U) In a big institution like NSA, we spend a considerable amount of time preparing for the future - as uncertain or difficult to predict as it might be. But deep below the surface there is one ingredient which I believe is the key to the health of the institution and which overrides all the ingredients of our strategic plans (vision, goals etc.) - optimism. With it, together with an understanding of mission, we will set the vision and accomplish the goals we set out for ourselves. Without it, we will fail. The same holds true for the critical subelements of the institution - including cryptanalysis.

(U) What optimism is is hard to pin down exactly. It's not constant. It varies from one individual to another and from time to time within oneself. It's a feeling, a mental state, which is influenced by rational understanding. In the end, it's a way of life, shaping our assumptions and expectations. The debate I overheard in 1982 is not too different from debates still taking place today. The technology details are different, but it's still about what the future will bring, and there are still optimists and pessimists debating the issue.

~~(FOUO)~~ Here's the way I think we will succeed. Those who believe we will succeed will contribute their diligence and their creative problem-solving abilities to overcome the information security systems we target. They will avoid ruts. They will remember, it's NOT academic. They will apply the appropriate tools in the CA bag of tricks, or they will invent new ones. In particular, any one aspect of our cryptanalytic skill set will die only if they let it become irrelevant. And no one person, nor even one Agency, will do it alone.

(U) The problems will get harder and harder from a classical point of view. We are no longer the center of the cryptographic universe. Therefore, we can't expect to have the same advantages in that universe. As a player amongst players, we will need to open our windows, lower our moats, and get acquainted with the rest of the information security world. Only by understanding what's out there can we hope to have any advantage. So, as the problems get harder, we will change our stance.

~~(FOUO)~~ Every generation since the beginning of time has faced unsolved problems, many of which were eventually solved. Unsolved is a lot different than unsolvable. Unless you can prove something unsolvable, why give up on it? Cryptanalysis is a multifaceted discipline which

(b)(3)-P.L. 86-36

has adapted incredibly well over the years. Most often, it works by recognizing a weak link in an otherwise sound system. We need to analyze systems and understand the links be they mathematical intricacies, software implementations, hardware quirks, or human tendencies. So far, progress hasn't stopped, and I don't believe it's going to on our watch. Change, however, is a given. It's healthy to spend some time considering the future, but it's vital to find a way to embrace its challenges with enthusiasm.

(U) By the way, those who don't believe may find arguments which convince themselves we can't succeed. But, time and will will tell.

(U) Think for a second about where you fit on the spectrum of belief in our continued cryptanalytic success, and relate that to your personal accomplishments in the last couple years - it might tell you something!

"""""""

[redacted]

3b. (U) Call for Suggestions for KRYPTOS Distinguished Members (U)

(U) Each year the KRYPTOS Society selects retired individuals as Distinguished Members of our organization. The purpose of the selection is to honor individuals who have made significant contributions to the field of Cryptanalysis and CA-related disciplines throughout their careers. The individuals selected have inspired us through their cryptanalytic accomplishments, supervision and management.

(U) We invite you to provide the Nominating Committee with suggested names for consideration. Please include your reasons for your suggestions.

(U) Following are some guidelines which the Nominating Committee will use:

1. In selecting individuals for distinguished membership, KRYPTOS strives to honor recent retirees or sterling figures from the past who have made their mark in some way on the cryptanalytic community.

2. Because KRYPTOS was founded to further the interests of cryptanalysis, emphasis should be placed primarily on cryptanalytic work done by the individual, but with consideration also given to cryptomathematics and cryptoprogramming contributions.

3. The individuals should have had actual hands-on experience in CA during a major portion of their careers. Cryptanalytic management experience, to the extent that the individual demonstrated dedication to the advancement of cryptanalysis, should also be considered.

(FOUO) Previously selected Distinguished Members are listed on the NSA WEB: [redacted]

(FOUO) Names should be forwarded to [redacted] by 5 June 1998. Please use "KRYPTOS Distinguished Members" as the Subject line of your email. (b)(3)-P.L. 86-36

//

4. (U) COMMUNITY NEWS:

4a. (C-CCO) Call for Abstracts: NSA's Computer Communication Working Group -- C2C Target Development

(C-CCO) NSA's Computer Communication Working Group (CCWG) announces the Sixth Annual Conference on Computer Communications to be held on October 26-29, 1998 in the Friedman Auditorium. On October 30, 1998 there will be demonstations and discussions in the Headquarters Building, room 9A135. This year's conference theme is "C2C Target Development."

(U) Participation in the conference is open to all fully cleared (b)(3)-P.L. 86-36

[redacted]

First and Second Party personnel and NSA contractors. Presentations and demonstrations from NSA DO, DI, and DT organizations, NSA contractors, First and Second Parties, and other intelligence agencies are solicited.

(C-CCO) This year's conference focus areas include:

* C2C Target Development Process -- Focus on the target development process and problems from the perspective of NSAW, field sites, and Second Parties,

* C2C Target Development Methodology -- Focus on techniques, training and tools currently being used for C2C target development.

* C2C Future Directions -- Focus on technology and research that relates directly to C2C processing and target development.

(FOUO) Please send abstracts (1-2 paragraphs) to [redacted] by 15 July 1998. The CCWG will notify authors of acceptance by 1 September 1998.

(b)(3)-P.L. 86-36

(C-CCO) This conference provides opportunities for information exchange and networking among a broad audience, to include intelligence analysts, SRTD analysts, collectors, engineers, computer scientists, mathematicians, signals analysts, and others involved with intercept, forwarding, processing, analysis, and reporting of intelligence from computer communication systems.

(S-CCO) Definition of C2C: C2C is any exchange of information between two or more computers or applications programs. This exchange can consist of multiple data types such as fax, bulletin board or web accesses, x-windows sessions, e-mail with attachments, or a more complex collaboration event with video, voice, images (whiteboards or graphics) and data (shared applications) being simultaneously exchanged among two or more communicants. It can also consist of automatically generated network maintenance information such as routers exchanging information about communications paths. Furthermore, this information exchange can occur across many different protocol structures and multiplexing schemes as it transits through the global telecommunications networks from one communicant's computer to another. [redacted] The CCSG welcomes briefings on how these topics relate to C2C target development.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(C-CCO) This year, the CCWG wants to work with presenters to develop a series of briefings that will engage an international, multi-agency audience in the various aspects of the C2C target development. The CCWG especially would like to see several case studies describing different aspects of the same target development problem. If you can provide part of the picture or recommend other organizations that can round out the picture, we want to hear from you!

(C-CCO) If you have an intelligence target communicating on a computer-to-computer network that you are trying to exploit, and you are working to resolve problems, then what you are doing may solve problems for other organizations. The past conferences have established a productive forum for dissemination of information and sharing of ideas. This is an opportunity for learning and teaching

(b)(3)-P.L. 86-36

[redacted]

through a unique briefing discussion format, conveying to your counterparts your successes, frustrations, failures, insights and solutions. Contributions may be up to TOP SECRET CODEWORD. No special compartmented materials are permitted.

~~(C-CCO)~~ Authors are invited to submit a short general paragraph to the CCWG conference committee describing a talk, visual presentation or demonstration. Please specify how much time you will need, either 15, 30, or 45 minutes. All presentations should be aimed at the general NSA audience. Themes for discussion may include, but are not limited to the following general problem topical areas:

* Successful analysis and targeting strategies.

* The status of network target development efforts and what successes have come from the SRTD and the OPI working together.

* Tools and techniques being used for target development.

* Interagency collaboration.

~~(FOUO)~~ CCWG Conference Committee

Co-Chairs:

Members:

[redacted]

(b)(3)-P.L. 86-36

4b. ~~(FOUO)~~ History: "Women in Cryptology" -- Speech presented by Miss Ann Caracristi, Former D/DIRNSA, at NSA on 6 April, 1998 in commemoration of Women's History Month

(U) My first trip to a museum was when I was about six years old. I was taken into New York to visit the Museum of Natural History and I can still remember my fascination with the mummy cases covered with hieroglyphs -- and I can remember my sense of amazement and awe looking up at the huge dinosaur skeletons that were installed in large, high-ceilinged rooms.

(U) Little could I have known that I would spend a career involved with the modern-day equivalent of hieroglyphics. Nor that I would reach the point where I could be described as one of NSA's living dinosaurs!

~~(FOUO)~~ Well, our National Cryptologic Museum is not yet quite up to Metropolitan Museum standards -- but we have high hopes! And I think we owe a great debt to Ken Minihan for his enthusiastic, unfailing support -- and to former Director Bill Studeman for taking the steps necessary to acquire the Colony Seven property to house the public museum -- and to Gen. John Morrison for forming the Museum Foundation

(b)(3)-P.L. 86-36

[redacted]

-- and to many volunteer docents and Foundation Committee members who are working to help the Museum become the "best institution of its kind in the world."

(U) We have described the three interacting missions of the Museum to be:

to commemorate the accomplishments and contributions of individuals and organizations;
to educate both professionals and the public about cryptologic activities and their value to the nation; and
to stimulate the imaginations of those who visit and participate in Museum programs.

(U) I think it is most fitting that the Museum will commemorate the role of women as a vital part of the story of cryptology. I am honored to be here today for the dedication of this display.

(U) Historical artifacts, models and pictures are, of course, basic to the museum collection, but creating and explaining the "culture" -- the feel of the time, describing the personality of the people and how they worked together and how they felt about being a part of the mission -- is very difficult.

(U) Each of us who was a participant is likely to have a narrow and perhaps distorted view. Memory is faulty -- even contemporary recollections can be suspect (you may have noticed comments about Robert Reich's book, _Locked in the Cabinet_). Fortunately, trained historians, like intelligence analysts, are skilled at putting conflicting stories together to arrive at something close to "ground truth."

(U) I will try to convey some sense of what it was like "way back then" during WWII -- but remember, it is only one person's experience. However, lots of researchers and historians are now able to examine the declassified records, so the documented record is becoming more and more balanced.

(U) I came to Washington in June, 1942, within a week of graduation from college. I knew only that I would be working for a branch of the Signal Corps, a branch that had something to do with something called cryptography. I came because, like almost everybody else, I wanted to do something for the war effort. It was the first opportunity that came along. I was never interviewed by anyone. It seems that my college dean had given my name and the names of two of my classmates, Kitty and Katie, in response to a request for candidates. We were accepted. And considering it something of a lark, we set off for Washington.

(U) To really get the flavor of Washington in 1942 you ought to read David Brinkley's marvelously entertaining -- and wonderfully accurate -- description in his book, _Washington Goes to War_. It was a hot, humid, overcrowded city, in confusing transition from being a sleepy southern city to becoming a war-driven boomtown. According to Brinkley, more than 70,000 new people arrived in the first year after Pearl Harbor alone. And Kitty, Katie and I were among them.

(U) Finding a place to live was a real problem. Somehow we managed to get a room in what had once been the Armenian Embassy, where we stayed until we lucked into an apartment in Arlington.

(b)(3)-P.L. 86-36

(U) Nowadays the military talk a lot about "tempo" -- they mean operational tempo. In WWII Washington, the word "tempo" described buildings: the temporary buildings we worked in and the buildings many of us lived in, not only military personnel but large numbers of the women who were recruited as clerks and typists for all the many civilian war agencies --- OPA, OWI, OCD -- and for the SIS, the Army Signal Intelligence Service. The Munitions Building on the mall was one of a series of "tempos" left over from WWI. And that's where we reported for duty.

(FOUO) That first day was my only visit to the spaces where William Friedman and his remarkable team had broken the Japanese PURPLE machine and had developed the enciphering machines and devices that were to protect U.S. communications throughout WWII. That early team included several women, among them Wilma Davis (then Zimmerman), Dee Sinkov (Abe's new wife), and Mary Jo Dunning, a statistician. Although she was not formally a part of the team, William Friedman's wife, Elizebeth, was very much in the background as a cryptologic pioneer in her own right, publicly acknowledged for her role in helping the Coast Guard run down Prohibition's largest ring of rumrunners.

(FOUO) Our visit to the Munitions Building was brief. We were sent off to a classroom at George Washington University, where we were to spend a few weeks studying Mr. Friedman's series of books on cryptography. Our teacher was Evelyn Ackley, a former professor of mathematics from Skidmore College, who was working through the Friedman _Elements of Cryptanalysis_ right along with us, maintaining her lead by staying one chapter ahead. We spent eight hours a day working problems in substitution and transposition and learning about Playfair squares and other such encryption schemes. But our "graduation," it turned out, had more to do with when we could move to Arlington Hall than how skillful we had become at finding solutions.

(U) So one day in July we joined the group at Arlington Hall, the former girls' school taken over by the Army, just as the Navy had taken over Mount Vernon Seminary in NW Washington. It can't be denied that the early cryptologists had a knack for locating good real estate.

(U) Attractive as the location was, however, it was very hot in July. And I was assigned to a group that was working on the Japanese Army and water transport systems. We were located under the eaves on the top floor of the school building. There were bathrooms between every two of the former bedrooms, but the water was turned off so it was safe to use the bathtubs as filing cabinets for the vast stacks of intercepts we needed to attack. Of course there was no air conditioning at Arlington Hall, or in the Navy's buildings, except in the "machine rooms" where IBM and special-purpose analytic and decryption devices were located. The cool air was for the machines, not the operators!

(FOUO) When the Lt. Col. in charge told me I was to be assigned to the Japanese problem, I was astounded. I certainly didn't know Japanese -- and, thinking of my training in Mr. Friedman's Cryptanalysis I and II, I couldn't think I'd be very helpful in working on a problem without knowing the language. "Don't worry," he said. "we'll teach you."

(U) Well, what they taught me was how to sort and edit the volumes of enciphered messages that had been intercepted by Morse operators in the Signal Corps units scattered throughout the West Coast and the Pacific. Later, many of those intercept positions would be staffed by WACs in

(b)(3)-P.L. 86-36

the Army's Second Signal Service Battalion.

(U) Our assembly-line routine was: SORT, EDIT, PUNCH. Punch operators, women civilians -- and later, WACs -- would convert all that material into punched cards that could then be sorted on IBM tabulators and the results listed for study.

(~~FOUO~~) Talk about "one team, one mission!" Our group of about 15 people included our civilian leader, Al Small, who had been at the Munitions Building with Friedman, a just-out-of-OCS 2nd Lt. who happened to be a nephew of Frank Lloyd Wright, several GIs waiting to go off to Ft. Monmouth for Officer Candidates' School, Wilma Davis, and a couple of other newly arrived civilian women like me. We all pitched in to sort and edit. And while we did that humdrum work we talked about what to look for. It was clear that we all could have a voice in making the plan of attack -- any good idea was accepted and put into effect immediately. Newcomer Jeanie Cocroft was the first to come up with a way to "de-dupe" the traffic, which saved a lot of punch time.

(~~FOUO~~) It was known that our traffic was enciphered manually. The Japanese were using additive from pads of key combined with groups from codebooks. The trick was to figure out the indicator systems, line up messages that came from the same key pad (overlaps), recover the plaintext code, break the codebook and translate the message. In due course this process would engage a work force of several hundred civilians (mostly women), a few officers (men) and a large group of Japanese linguists, mostly enlisted men, working in three shifts around the clock, seven days a week.

(~~FOUO~~) By 1943, large numbers of women had been recruited from high schools and colleges in the south to work at Arlington Hall. Many of them would live in the newly built group of "tempo" quarters called Arlington Farms. They were the clerks, sorting and handling traffic, and they were the overlap readers, posting messages on large worksheets, recovering keys and producing decrypts to send off to the translators. Some -- Charlotte Girhard, Nancy Maldon, Gene Raymond -- became traffic analysts, working with the largely military group who were reconstructing the Japanese Army Order of Battle. Some worked as cryptanalysts -- as I did. In my section only a few of the new women recruits were mathematicians -- Anne Solomon was one. Except for those training to be teachers, very few women were encouraged to study math in the pre-war period. (Remember that prior to WWII the number of fields in which women could hope to find professional jobs was very limited: teaching, nursing, merchandising were about it.)

(~~FOUO~~) Fortunately for cryptology (if not for the educational establishments of the early 1940's) women teachers turned out to be a wonderful source of talent for many of our jobs, including math and foreign languages (mostly French, Spanish and German, however). These were women who would work on the German and European targets in what was, to me, the "other" part of SIS -- the part run by Col. Frank Rowlett. Our Japanese linguists were mostly military and mostly men, who were selected from colleges around the country, drafted, and put into immersion courses at Boulder, Colorado and at Syracuse University. A few had been missionaries -- or came from missionary families that had lived in prewar Japan.

(U) It was generally believed that women were good at doing tedious work and, as I had discovered early on, the initial stages of cryptanalysis were very tedious, indeed. So women were recruited not

(b)(3)-P.L. 86-36

9/24/2010

only to free up men to go overseas, but to do the jobs that they were assumed to be most suited for. It's probably hard to understand why young women would come to Washington to work for $1,440 a year (yes, that's fourteen hundred and forty dollars a year, or $1,620 if you had a Bachelor's degree and $1,800 for a Master's), but these were women accustomed to depression wages. And teachers' wages were notoriously low even in good times. And these were 1942 dollars!

(~~FOUO~~) Those of us who considered ourselves Arlington Hall pioneers -- who moved in during those first few weeks -- have special memories. We remember the famous "guard force" made up of freshly drafted high-IQ GIs (draftees were selected for SIS on the basis of their test scores), GIs like Arthur Levenson and Arnold Dumey, who had never held a gun before in their lives, drew every third or fourth night and had to patrol the Arlington Hall grounds. There were many stories, some of them true, about guns going off accidentally in the guardroom. We remember watching "A" Building being built in record time. The long, unpartitioned "wings" were outfitted with rows of old dilapidated desks and tables scrounged from heaven-knows where and populated with the ever-growing work force. The Cafeteria Building and "B" building came next.

(U) David Kahn says that in June, 1945 we were up to about 10,500 at Arlington Hall: 5,500 civilians, 4,500 enlisted (1,500 of them WACs) and 800 officers. I don't know how many of those civilians were women -- but I suspect it was about 90%.

(~~FOUO~~) Security was a matter of great concern then and it led to extraordinary compartmentation, which in turn meant that very few of the people at Arlington Hall -- or in the field -- understood what was happening outside of their immediate area. Need-to-know was strictly observed. My college friend Kitty had ended up being assigned to the reporting shop headed by the legendary Dr. Julia Ward (a former dean at Bryn Mawr), so I was aware at least that translations (mostly) and reports were being published and distributed. And Katie ended up in a COMSEC unit, so I knew that there was a part of the SIS that worried about the key diplomatic system called "PURPLE" which was being read. But it wasn't until V-J Day that I ever saw a translated PURPLE message.

(U) As the work force grew and the production process became somewhat more coherent, the output became more timely and valuable. But the organization was still a "work in progress". There were times when we marveled that anything useful was produced. It seemed, miraculously, to come out right despite the confusion (even chaos) of what seemed to us loose or sometimes nonexistent management and organization. But morale was high. We had a clear mission -- WIN THE WAR -- and, since most of us expected to go back to "real life" at the end of the war, we did not much feel the need to compete for promotions or worry about turf. On the whole we regarded our activities more as sport than business. We were serious and dedicated (many of us worked ten-hour days) -- but we enjoyed working together and playing together. We had picnics and softball games, a choir and an amateur theater group. We went to the movies at Ft. Meyer. We saw "Oklahoma" when it opened at the National Theater.

(~~FOUO~~) The chief of the Japanese military branch was Col. Solomon Kullbach. Kully was one of the "greats," hand-picked and trained by William Friedman. Despite his wartime military rank, he was at heart a civilian professor of mathematics, far more interested in cryptanalysis than in organizational charts. Nevertheless he crafted an organization

(b)(3)-P.L. 86-36

9/24/2010

that by early 1945 was reading nearly every message transmitted by the Japanese military -- usually within hours of transmission, and sometimes long before the intended recipient read them. We were much better than the Japanese at dealing with garbles and encipherment errors.

(~~FOUO~~) Kully didn't hesitate to put women in charge. Wilma Davis, Delis Sinkov, and Mary Jo Dunning were all section chiefs.

(U) Meanwhile, across the Potomac, at the Naval Communications Annex, Navy cryptanalysts were successfully exploiting the German Navy ENIGMA, using U.S. versions of the British Bombe devices. By far the largest number of the mostly military work force were WAVES. Some 3,000 were stationed there by early 1944, most of them involved in the 24 hour, seven day a week operation of the Bombes.

(~~FOUO~~) Among the civilians who played important roles in Navy cryptanalysis were Agnes Driscoll and Polly Budenbach. But most of us at Arlington Hall weren't aware of their successes until after the war when, at long last, the Army and Navy cryptologists did become one team.

(U) Looking back, we now know that the WWII cryptanalysts played a central role working against the Japanese army and navy. The Battle of Midway, the success of MacArthur's island-hopping strategy, the U.S. ability to decimate the Japanese fleet of supply ships, the shootdown of Admiral Yamamoto's plane -- all were guided by intelligence coming from successful cryptanalytic attacks. And in the Atlantic, U.S. and British exploitation of ENIGMA led to the ultimate elimination of the German submarine threat.

(U) Without the women working at Arlington Hall, at the Naval Communications Annex, and in the intercept sites of the Second Signal Service Battalion, the massive production of decrypts and translations would never have been possible. Most of these women did go back to "real life" at the end of the war -- and these, now mostly nameless, are the heroines of the Second World War.

(~~S~~) Along with many, many others, I departed after the war and went to work in New York. But I couldn't resist the temptation to return when I was invited back a year later. Now it was the Soviet Union that was the threat -- and I came to work in Oliver Kirby's Russian division. Carry Berry was my new boss. We worked on the Soviet military problem, but in the front of our B Building wing was the VENONA group that we now know so much about -- thanks to the work of the NSA Center for Cryptologic History and the Agency decision to declassify the story. In the ceremony honoring the VENONA team of early heroes and heroines, Miss Gene Graybeel (a school teacher recruit) was acknowledged as the person who started the VENONA project in 1943. Among the 35 people listed, 17 were women.

(U) No discussion of the role of women in cryptology can overlook the role of General Canine, the first director of NSA. He was the one who set the standards for many things: the look of the workplace -- he finally got rid of the prewar furniture; the look of the work force -- he insisted that we dress like professionals. Coat and tie were in; bobby socks were out. But most of all he insisted on fairness in rewarding performance. He went to bat to get a higher grade structure for all NSA civilians -- but he was especially insistent that deserving women be considered for promotion to what were then the senior grades of GS-13 and GS-14. (After the war there were only

(b)(3)-P.L. 86-36

three GS-15 cryptologists: Kullbach, Rowlett and Sinkov. A few other returning former officers converted to GS-14 and a few more to GS-13.) There were no women civilians above the grade of GS-12 in either Army or Navy cryptology. General Canine saw to it that that particular glass ceiling was broken.

(U) It is obvious that there are many more stories to tell about cryptologic success (and failure) during the period of the Korean War and the War in Vietnam, and about the early years of the Cold War, as more and more intelligence and cryptologic history is made available for public release. And as this happens, I think we can expect to learn more and more of the contribution of women to cryptology at NSA and in the service cryptologic elements.

(~~FOUO~~) But I suspect that we are fast approaching the point in our society -- and in the world of cryptology -- where the "we and they" of men vs. women in the workplace becomes less of an issue. The presence of senior women in all parts of the business at NSA today -- from research and engineering to computer programming, to the development of new secure information systems, to logistics, training, advanced cryptanalysis, translation, transcription, analysis, and reporting -- is taken for granted, as are the many women serving as NSA representatives in intelligence centers and collections units around the world. Even the fact that we have today (I'm delighted to note) another woman D/DIR, is not too remarkable, nor is the fact that there are today women in charge of major organizations throughout the Agency.

(U) Finally, let me say that I know that I am one lucky person -- first, because I was able to be here in the early years to share in the excitement and fascination of our accomplishments -- but also because, in retirement, I'm still able to share many of your TOP SECRETS. I know something of how important your work continues to be today. I know that all of you, women, men, civilian and military, are making history at this very minute. And sometime in the future, maybe thirty or forty years from now, the Center for Cryptologic History will be writing your story and their diligent staff of historians will be helping the world famous National Cryptologic Museum prepare a display of the accomplishments you have been a part of. So my message to you is "enjoy the sport," continue to solve the hard and challenging problems -- and don't forget to share your memories with the historians.

"""""""

On this page, of course, there is no such mediocrity as that... Instead, try this extended filler chain, where each blank in a series must make a word or phrase, when paired with the letters in brackets on either side.

[TOU]___[TER]___[COR]___[TER]___[FALL]___[SIDE]

(U) Solution:

[TOU]CAN[TER]RAN[COR]SET[TER]RAIN[FALL]OUT[SIDE]

(Other solutions are possible.)

~~(FOUO)~~ Solutions were provided by [redacted]

5b. (U) May Puzzle - Triple Play (courtesy of El Tigre)

(U) The trios of letters below can be re-ordered (without rearranging the order of the letters within the trios themselves) to form a quotation and the name of its author. The lengths of the words and the punctuation for the quotation have been given to help you along.

ARO ATC ATO COM CON CTO DEN DIF EAR ECO EDT EEA ETI FDI FIC FOR
GDE HAV HWH IND ING ION LEA LLY LNE MOS MYM NGI NIS NOR NTI NUA
OPL OPO OWA PAR PIN PUL REA RPE RYT SNO SPE TAB TCH THE THE THE
TIN TIS TOW TRA TTH TTO TUN TYO UEA ULT WHA

(8 2 7 7, 3 4 13 6 2 7 2 3 3 9 4 2 5 4 3 3.
2 2 4, 3 6 9 4 2 6 2 5 4 5 6 3 6. - 5 6)

~~(FOUO)~~ Send all solutions, as well as puzzle submissions, to [redacted]

6.(U) EDITORIAL CORNER

REMINDER: (U) Submissions for the June issue are due by May 28.
PLEASE NOTE: (U) All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION-MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

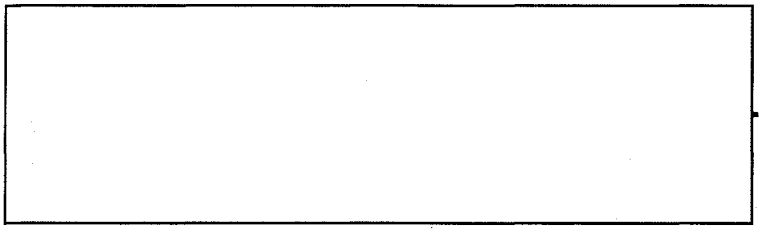
[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

[redacted]

(b)(3)-P.L. 86-36



(b) (3)-P.L. 86-36

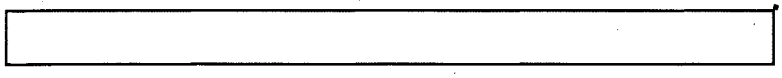
(b) (3)-P.L. 86-36

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

(b) (3)-P.L. 86-36



TOP SECRET/COMINT

~~(C)~~ *POC:* [redacted] *info*
(U) *Last Modified: 10/30/2002 11:42:23*
(U) PE EXTERNAL PAGE

(b)(3)-P.L. 86-36

```
*********************************
*        TALES OF THE KRYPT     *
*********************************
```

June-July 1998

//
****

++
//

(U) TABLE OF CONTENTS:

1. ~~(FOUO)~~ Perspective: by [redacted] Chief, Z07.

2. (U) Calendar of Events

3. (U) Cryptanalysis Career Panel (CACP) News

   3a. (U) CACP Certifications, Personnel Changes and New Interns

   3b. (U) CA Technical Track Titles Awarded

   3c. (U) 1998 Professional Qualification Examination Statistics

4. (U) KRYPTOS Society News:

   4a. (U) First Annual Technical Talk Contest

   4b. (U) Call for Literature Contest Papers

   4c. (U) Call for Nominations for the Peter Jenks Award for Community Service

   4d. (U) Call for Nominations for the Norman Roberts Award for Junior Cryptanalyst

   4e. (U) Call for Volunteers to Produce KRYPTOS Society Video

   4f. (U) KRYPTOS Society President's Report Now Available on the NSA WEB

5. (U) Community News

   5a. ~~(FOUO)~~ Military Cryptolinguist Training Program (MCLTP) by [redacted] MCLTP Manager

   5b. (U) International Affairs Institute (IAI) 1998 Essay Contest

   5c. ~~(FOUO)~~ Z Women's Council Notes, by Chair [redacted]

   5d. ~~(FOUO)~~ Center for Cryptologic History Publication Reaches New Audience by Sharon Maneki, S542, Center for Cryptologic History

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

6. (FOUO) Puzzles
by [redacted]

6a. (U) Answer to May Puzzle

6b. (U) June-July Puzzle

7. (FOUO) Letter to the Editor: "What Am I Talking About?!?!?"
by [redacted] M3

8. (U) Editorial Corner

(b)(3)-P.L. 86-36

****
//////////

1. (FOUO) PERSPECTIVE - Each month this newsletter features the perspective of a Senior on a CA topic of his/her choice. This month we are pleased to feature the thoughts of [redacted] Chief, Z07.

(FOUO) I am very happy to have been asked to write this note to you today. I am currently Chief Z07, Math Career Panel Chairman, member of the Senior Technical Track Board, member of the Senior Technical Review Panel, and co-leader of one of the Z07 Research Pods. All this makes for a pretty busy day, so it is a pleasure to be forced to take a little time to reflect on things.

(FOUO) I have had plenty of experience here at NSA to help me in this. I started out in the predecessor to the Cryptomath program, had many years experience in the old G4 and in A54, a tour at GCHQ, a tour at LaJolla, attended SCAMPs at Princeton, LaJolla, and Bowie, numerous interesting TDY's, have been on the CA Career Panel and the Math Career Panel, and was President of KRYPTOS.

(S-CCO) Most importantly, it seems to me that in our technical work we are living in the best of times so far. We have great problems to work on, more computer power and better access to data than ever before. The problems are of all kinds, but they all demand our problem-solving skills. The traditional crypt problems are as important as ever and now we also have new kinds to work on, such as software and hardware reverse engineering, network protocols and applications, software encryption, authentication, software systems with embedded encryption and with various kinds of non-cipher that still need analysis.

(FOUO) The keen sense of observation and superior problem-solving skills are all we need for many tasks, but increasingly we need to know more of how to exploit the technical tools that we have and the technical tools that our targets have. Our cipher text doesn't come printed on a piece of paper any more. It comes embedded in some kind of communications protocols, compressed, in some office application. We sometimes hear comments about our being insular, that we need to get out of the "box", but this isn't anything we have to do artificially--we are driven to it by new technology. Actually in the bigger picture, this is the essence of cryptanalysis, out-of-the-box thinking to solve problems.

(U) How could we be happier? We have great problems and that is what we want most. However, there are some problems with the problems. In terms of technology we have to work pretty hard just to keep up. This is a new idea, at least for me. In the past, you could go from a small

(b)(3)-P.L. 86-36

[redacted]

base of reasonably static knowledge, and with a lot of deep thought, come up with elegant, simple solutions. I think about writing FORTRAN programs to be punched onto card decks and handed in over a counter. Now the rate of change is immensely greater and the amount of knowledge pouring out is equally huge. In an attempt to make every action you take be simple, the modern trend is for you to program by combining a large number of supplied routines. You don't know how they do what they do and you don't need to. But you do need to know about a lot of them. When you go to the bookstore, instead of that thin FORTRAN manual, you see rows of 500-page $50 paperback books on this year's computer languages, while last years $50 computer language paperbacks languish on the remainder table for $5.98. What is new is the huge volume of knowledge which is so rapidly obsoleting prior knowledge and that breadth is replacing depth.

(U) We have to find ways to cope with this change within the large bureaucracy that is NSA. We have to find ways to acquire this knowledge in a timely fashion, to purchase books, take classes, go to conferences, and have reasonable access to the Internet. We have to be able to obtain and experiment with new software products and computer equipment. We have to be able to rapidly adapt our programs to new realities. The world is going ahead whether we are or not.

(U) This is a very unsettling time for us as NSA employees. We have an activist DS that is throwing all kinds of things at us: P3, SPECTRUM SkillsMap, IDP, Multirater Assessment, the new promotion process. We don't know how all this will affect us, but change is unsettling, especially when you don't seem to have any control over it.

(U) I am proud to be a part of NSA and like the culture that we have as cryptanalysts, where quality counts. I feel we have a structure that, in general, recognizes the value of technical people and rewards them. Being somewhat conservative, I'm not sure I like all of the new ideas in personnel management. I don't like the phrase "best commercial practice," because I don't think that is NSA. And I don't see any reason to artificially force our objectives into something that we can measure.

(FOUO) I am reminded of when I was a team chief in A54. [redacted] then Chief of A541, had asked me for my team goals, accomplishments, and shortfalls for that year. I said my goal was to solve X. He said, "No, you have to give me a set of goals that you are sure you can accomplish, like process N thousand extracts." Well, I didn't like it but I gave in. A short time after that [redacted] did some magic and solved X! We changed our path of course and I doubt that we processed all those N thousand extracts.

(b)(3)-P.L. 86-36

(U) I want goals that I can try my best to achieve and be thrilled if I can make. I think that's the way we have achieved the level of technical excellence we have at NSA.

(U) If I am allowed to give some advice, it would be to be a part of the mainstream of your office. Have the self-confidence to take the time to think deeply about those great cryptanalytic problems you are working on. You will do marvelous things. Keep learning. There are lots of ways to learn. Each new problem is an opportunity to learn. Look for opportunities to try new things. Find out what you are good at and what you are not so good at. Accept responsibility and give back to the cryptanalytic community.

(b)(3)-P.L. 86-36

[redacted]

2. (U) CALENDAR OF EVENTS

Jun 29 - Aug 28	(U)	SCAMP at Princeton/Cheltenham
Jul 31	(U)	Deadline for Nominations for First Annual Technical Talk Contest (See 4a.)
Jul 31	(U)	Deadline for Nominations for Literature Contest Papers (See 4b.)
Jul 31	(U)	Deadline for Nominations for the Peter Jenks Award for Community Service (See 4c.)
Jul 31	(U)	Deadline for Nominations for the Norman Roberts Award for Junior Cryptanalyst (See 4d.)

PLAN AHEAD

Aug 8	(U)	CMI/KRYPTOS Society Night at the Bowie Baysox
Sep 11	(U)	CMP Graduation, Friedman Auditorium, 1300
Oct 26-29	(~~C-CCO~~)	CCWG Conference on Computer Communications: C2C Target Development
Nov 2-6	(U)	CONSCRYPT '98 at CSE
Dec 2	(U)	A5 Reunion, Blob's Park

3. (~~FOUO~~) Cryptanalysis Career Panel (CACP) News by [redacted] Assistant Executive, CACP

3a. (U) CACP Certifications, Personnel Changes and New Interns

(~~FOUO~~) Congratulations to the following newly certified cryptanalysts!

[redacted]

(~~FOUO~~) The CACP welcomes the following:

[redacted] as Chairman of the CA Career Panel.

[redacted] as Members of the CA Career Panel.

[redacted] as Members of the Technical Paper Evaluation Board.

[redacted] as Member of the Computer Program Evaluation Board.

[redacted] (b)(3)-P.L. 86-36

[redacted]

[redacted] (b)(3)-P.L. 86-36
as Member of the CA Technical Track Review Panel

~~(FOUO)~~ The CA Intern Panel welcomes its newest intern, [redacted] who was hired by NSA in March.

3b. (U) CA Technical Track Titles Awarded

~~(FOUO)~~ Congratulations to all recently titled members of the Cryptanalysis Technical Track.

MEMBERS

[redacted] (b)(3)-P.L. 86-36

SENIOR MEMBERS

[redacted]

MASTER

[redacted]

3c. (U) 1998 Professional Qualification Examination Statistics

~~(FOUO)~~ The annual CA PQE was given on May 5 & 6. [redacted] aspirants took the exam, and [redacted] passed. The passing score was 9, out of a possible 16 questions (8 given each day). (b)(3)-P.L. 86-36

//

[redacted]

4. (U) KRYPTOS Society News:

4a. (U) First Annual Technical Talk Contest

(FOUO) The first annual Technical Talk competition seeks to recognize the best technical presentation on a subject relating to cryptanalysis or one of its related disciplines. The contest is open to all personnel at NSA, GCHQ, CSE, DSD, GCSB, to personnel on field assignment, and to retirees (consistent with security considerations).

(FOUO) Talks presented in the timeframe 1 July 1997 to 30 June 1998 are eligible for the competition. All recorded KRYPTOS talks given in that timeframe will automatically be considered (with presenters' permission). All talks must be videotaped and last at least 30 minutes. It is strongly recommended that entries carry a classification no higher than TSC. However, talks at the [redacted] levels will be accepted.

(b)(3)-P.L. 86-36

(FOUO) The judging panel will consist of three judges from NSA and one judge from GCHQ. The winners will be announced at the annual Fall KRYPTOS Society Luncheon, and prizes, whose nature is yet to be determined, will be awarded.

(FOUO) The judges will consider the following criteria:

- Is the talk an original discussion of a cryptanalytic subject? The talk should be a description of new work done by the presenter(s) or a survey of previous work giving proper credit.

- Is the talk presented in a manner which makes it easy to follow and understand? Is there a rapport between the speaker and the audience? Does the speaker demonstrate enthusiasm for the subject matter?

- Does the talk successfully serve as a vehicle for disseminating information about a relevant topic from the body of professional cryptanalytic knowledge?

(FOUO) Anyone can enter a videotaped talk with the permission of the presenter(s). Neither the author nor the submitter (if different) has to be a member of the KRYPTOS Society. If you have any questions regarding this competition, please contact [redacted]

(FOUO) To enter, please submit two copies of the videotaped talk, or indicate that the talk is available on videotape in the Z technical library, R51 library, or another similar repository, to [redacted] HQS, or

(b)(3)-P.L. 86-36

by July 31, 1998. Each entry should be accompanied by the following information: name and current organization of the presenter, title of talk, and classification of talk.

4b. (U) Call for Literature Contest Papers

[redacted]

~~(FOUO)~~ The annual KRYPTOS Society Cryptanalytic Literature Competition is now underway. The competition is open to all personnel at NSA, GCHQ, CSE, DSD and GCSB, to personnel on field assignments, and to retirees (consistent with security considerations).

~~(FOUO)~~ The papers may treat any topic in the broad category of professional cryptanalytic literature, including:

- operational cryptanalytic problems, either SIGINT or INFOSEC;

- cryptanalytic research;

- history of cryptanalysis;

- topics not of a direct cryptanalytic nature but clearly relating to cryptanalysis, e.g. computer support of a cryptanalytic problem or communication trends relating to cryptanalysis.

~~(FOUO)~~ The judges will consider the following criteria:

- Is the paper an original discussion of a cryptanalytic subject? The paper should be a description of new work done by the author(s) or a survey of previous work giving proper credit.

- Is the paper well written? Is the subject presented well? Is there a professional level of authorship, i.e. in style, grammar, spelling, format, and credit?

- Does the paper constitute an important addition to the body of professional cryptanalytic literature?

~~(FOUO)~~ Submissions may be written specifically for the competition. Papers written between July 1, 1997 and June 30, 1998 are eligible. It is strongly recommended that entries carry a classification no higher than TSC. However, papers classified [redacted] will be accepted, as will papers classified [redacted]

(U) Cash prizes totalling $300 will be awarded to first, second, and third place winners at the discretion of the judges. The judges may also deem a paper(s) worthy of honorable mention.

(U) Anyone may enter a paper with the permission of the author. Neither the author nor submitter (if different) has to be a member of the KRYPTOS Society.

(b)(3)-P.L. 86-36

~~(FOUO)~~ If you have any questions regarding this contest, please contact [redacted]

~~(FOUO)~~ To enter, please submit four copies of your paper to [redacted], by July 31, 1998. Each copy should be submitted with two cover sheets: the name(s) and organization(s) of the author(s) and title on one sheet, and only the title on the other to facilitate impartial judging. The competition results will be announced at the KRYPTOS Society Fall Luncheon in October 1998.

4c. (U) Call for Nominations for the Peter Jenks Award for Community Service

(b)(3)-P.L. 86-36

[redacted]

(U) Peter Jenks was the Founding Father of the Cryptanalysis Career Panel and the founder of the Cryptanalysis Intern Program. In recognition of Peter Jenks' dedication to the field of Cryptanalysis, the KRYPTOS Society established the Peter Jenks Community Service Award. This award may be presented annually to an individual in recognition of exceptional service and contribution to the CA community.

(U) Eligibility: potential award recipients include NSA/CSS civilian employees and military assignees who are active in the CA community.

(U) Selection Criteria: the President of the KRYPTOS Society and the Chairman of the Cryptanalysis Career Panel are responsible for providing the guidelines for recommending individuals for this award. The following basic selection criteria also apply:

- The service and contribution must be in the field of cryptanalysis and reflect efforts which exceed those expected in the performance of the job.

- Such endeavors may include, but are not limited to, serving on the CACP, as a KRYPTOS Society officer, as a member of a CA Technical Track Review Panel, as a judge for an award or contest, or designing and teaching a new CA course, coordinating technical talks, or other efforts which serve the cryptanalysis community as a whole.

(FOUO) Recommending Officials: any individual, or group of individuals, may nominate/recommend someone for this award. Such nominations, detailing the contributions the individual has made to the CA community, should be forwarded to the Secretary of the KRYPTOS Society Council, [redacted] by 31 July 1998.

(b)(3)-P.L. 86-36

(U) Procedures: this award may be given annually, but there may be one or more years in which the award is not given. A certificate of Honorable Mention may also be awarded, at the discretion of the KRYPTOS Society Council. Such awards will be made at the Annual KRYPTOS Society Luncheon.

4d. (U) Call for Nominations for the Norman Roberts Award for Junior Cryptanalyst

(U) In recognition of Norman Roberts' talent for nurturing the skills of junior analysts, the KRYPTOS Society established the Norman Roberts Award. This award may be presented annually to a junior cryptanalyst at NSA/GCHQ who has made an outstanding cryptanalytic contribution.

(U) Norman joined GCHQ in 1975 and won the respect and admiration of his colleagues for his innovative ideas, and particularly for his ability to train and inspire younger analysts, until his untimely death in July 1990.

(FOUO) Any KRYPTOS Society member may nominate any employee at NSA or GCHQ who has approximately five years' service as of 31 July 1998, and who has made an outstanding contribution to cryptology or a related discipline. (For a nominee with more than 5 years of cryptanalytic experience, the citation should explicitly draw the judges' attention to that fact, and explain why the nomination should be considered as falling within the overarching purpose of the Roberts award.) The

(b)(3)-P.L. 86-36

[redacted]

nominee does not have to be a KRYPTOS Society member. Integrees will be regarded as members of their host Agency. The nomination must include the names of the proposer and the nominee, together with an account of the work which attracted the nomination. It may be classified up to TSC. Nominations are due by 31 July 1998, and should be mailed to the KRYPTOS Society Secretary, [redacted]

[redacted] (b)(3)-P.L. 86-36

(U) The winner, selected by a joint UKUSA panel, will be announced in October and presented with a small engraved plaque.

4e. (U) Call for Volunteers to Produce KRYPTOS Society Video

(~~FOUO~~) If you are interested in working on the KRYPTOS Society's new video project, please contact [redacted] This is a unique and interesting opportunity to do a video from scratch -- theme, planning, design, drafting text, interviews, working with the NSA TV Studio, etc. If you have always wanted to do something like this and would like to portray Cryptanalysis and the Cryptanalytic Community to a large audience, here's your chance. Videotaping interviews with recent retirees will definitely be a part of this project. Call Therese now!

4f. (U) KRYPTOS Society President's Report Now Available on the NSA WEB

(~~FOUO~~) KRYPTOS Society President [redacted] report to the KRYPTOS Society Council is available for reading on the NSA WEB via link

[redacted] (b)(3)-P.L. 86-36

//

5. (U) COMMUNITY NEWS:

5a. (~~FOUO~~) Military Cryptolinguist Training Program (MCLTP)
by [redacted] MCLTP Manager

(U) First MCLTP Participant Begins Program in June

(~~FOUO~~) The Military Cryptolinguist Training Program (MCLTP), established in October 1996, is a 3-year intern-style program for the Services. The goal of the program is to enhance the cryptolinguistic skills of career military linguists through formal training and operational assignments. Selection is competitive, and participants can expect to be professionalized as a Cryptolinguist (or close to it) by the end of the program. Graduates of the program will then have a follow-on assignment at one of the RSOCs.

(b)(3)-P.L. 86-36

(~~FOUO~~) [redacted] a Chinese linguist, is the first participant to enter the program, with two other candidates scheduled to begin at the end of the summer. If you are interested in more information about the program, see NSA/CSS Circular # 40-19 or contact [redacted] MCLTP Program Manager.

[redacted]

5b. (U) International Affairs Institute (IAI) 1998 Essay Contest

~~(FOUO)~~ The 1998 International Affairs Institute Essay Contest is now underway and has as its organizing theme "Globalization." Under this theme, the following are possible, but not mandatory, areas of emphasis:

- Explore the technological challenges of achieving information superiority in a globalized world. What must we do to keep up?
- How should intelligence requirements be weighed against personal rights?
- Given developing economic interdependencies, who or what presents the greatest threat to the national security of the United States; is the National Security Community prepared to respond?
- What are the gains and risks of increased collaboration with partners?
- How can the National Security Agency maximize use of its decreasing resources to respond to ever-changing customer demands; when should we say no?

(U) According to Webster, an essay is a literary composition on a single subject, presenting the author's viewpoint. This is not a research paper so no footnotes should be included. Essays will be judged by a panel of five judges on content and style as follows:

Content, including adherence to theme and support of conclusion(s)	75 points
Style, including development of theme, vocabulary, grammar and spelling	25 points

(U) The contest is open to all NSA employees, both at headquarters and in the field, including military assigned to any NSA operations.

(U) Format:

- Essays can be 5-10 pages, doubled-spaced and in single column format.
- No graphics are to be used.
- The first page is a cover sheet with the name of the author, organization, phone number, room number, and title of the essay. The author's name and other identifying information should appear only on this page.
- The title of the essay should be repeated at the top of the first page of the essay.
- Essays should be sent to [redacted] by 14 August 1998. Those in the field may send their essay softcopy to [redacted] (b)(3)-P.L. 86-36

[redacted]

(FOUO) Classification: The overall classification of the paper may not exceed TOP SECRET CODEWORD. However, the paper may be unclassified.

(U) Prizes - First Place $300
Second Place $200
Third Place $100

(U) The IAI reserves the right not to award any or all of the prizes should there be no essays of sufficient quality in the view of the judges.

(FOUO) For further information, contact IAI Essay Contest Co-Chairs [redacted] or [redacted]

(b)(3)-P.L. 86-36

5c. (FOUO) Z Women's Council Notes, by Chair [redacted]

(U) The Z Women's Council would like to announce their new alias - zwc@z.nsa. Anyone who would like to address any questions or issues to the ZWC is invited to do so via this alias.

(S-CCO) The videotape of [redacted] Target Focus Group briefing given on 17 April 1998 is now available. If you wish to borrow this classified (TSC) video for viewing, please contact [redacted] ZWC Chair. Pat may be reached on [redacted] or by email - [redacted]

5d. (FOUO) Center for Cryptologic History Publication Reaches New Audience
by Sharon Maneki, S542, Center for Cryptologic History

(U) Each year, the Library of Congress selects a limited number of books to reproduce in Braille for distribution throughout the nation in its books for the blind program. In 1997, the Library of Congress selected a Center for Cryptologic History publication for the first time. Production was completed in May 1998. _The Quiet Heroes of the Southwest Pacific Theater: An Oral History of CBB and FRUMEL_, by Sharon Maneki, is now available in Braille to customers through the national network of libraries for the blind. (CBB--Central Bureau Brisbane--and FRUMEL--Fleet Radio Unit Melbourne--were COMINT organizations that supported General MacArthur in the Pacific during WWII.) [This publication won First Place in the 1996 Cryptologic Literature Contest.]

"""""""

ARO ATC ATO COM CON CTO DEN DIF EAR ECO EDT EEA ETI FDI FIC FOR
GDE HAV HWH IND ING ION LEA LLY LNE MOS MYM NGI NIS NOR NTI NUA
OPL OPO OWA PAR PIN PUL REA RPE RYT SNO SPE TAB TCH THE THE THE
TIN TIS TOW TRA TTH TTO TUN TYO UEA ULT WHA

(8 2 7 7, 3 4 13 6 2 7 2 3 3 9 4 2 5 4 3 3.
2 2 4, 3 6 9 4 2 6 2 5 4 5 6 3 6. - 5 6)

Solution:

"Contrary to popular opinion, the most uncomfortable aspect of [dieting] is not the continual need to watch what you eat. To my mind, the really difficult part is having to watch what other people are eating." -- Denis Norden

(~~FOUO~~) Solutions were provided by: [redacted]

[redacted]

(b)(3)-P.L. 86-36

6b. (~~FOUO~~) June-July Puzzle - Vexing Vocabulary
(taken with permission from the WEB pages of [redacted] and [redacted]
if you have an outside account)

(U) This is a puzzle combining elements of vocabulary and deductive reasoning. The object is to form a word in each row by placing one letter in the empty space in the middle column. Each letter of the alphabet must be used once and only once. Nearly all rows have more than one possible word that can be formed. For example, in the first row, the blank could be filled by a G, K, M, N, P, or V, giving the words OBLIGE, LIKED, MEDAL, LINED, PEDAL, or LIVED, respectively. All words must be formed with consecutive letters in the row (i.e., no skipping over letters), they must use the letter you put in the blank space (that letter can appear anywhere in the word), the word must be at least three letters long, and only standard, non-capitalized, non-foreign words are allowed (exceptions are allowed for British spellings :-)). Extra credit goes to anyone whose words are all at least five letters long - I don't have a solution for that, but it theoretically is possible.

1 OBLI_EDAL
2 PISC_REAL
3 NOVE_RUNK
4 AGEN_AGER
5 THIR_YALS
6 ADIN_USTO
7 TUXO_IOUS
8 OSTR_PEDE
9 OSTA_PINE
10 INCO_ERAS
11 APRE_TIGE
12 VALS_ACKS
13 SCAN_ONLE
14 INDA_GERT

(b)(3)-P.L. 86-36

[redacted]

15 FINE_ACTS
16 THER_ANTS
17 UPED_NTAL
18 CRAS_UEST
19 PRIN_LUXY
20 IMPO_ONER
21 GRAP_ICED
22 PENC_LORS
23 ALGE_RANT
24 PREL_DENT
25 OWAT_HARE
26 OBAC_LOGE

(~~FOUO~~) Send all solutions, as well as ideas for puzzle submissions, to [redacted]

7. (~~FOUO~~) Letter to the Editor: "What Am I Talking About?!?!?" by [redacted] (b)(3)-P.L. 86-36

(U) Okay, I give up. I'm throwing in the towel. This is the straw that broke the camel's back. I've HAD IT with acronyms.

(U) There is nothing particularly unusual about the acronym which has finally prompted me to write a short item for the _Tales of the KRYPT_. However, the extremely divergent meanings for individual acronyms has been hitting me with more and more force with each new office that I move to.

(U) I am assuming that most of the readers of _Tales of the KRYPT_ have backgrounds similar to mine. We've all spent most of our time working in DO; we are primarily analysts with some exposure to management; and, we have a CA or math slant to our work.

(~~FOUO~~) Well, given that background, what comes to mind when you see the acronyms AOR, LOB, MEPP and OTA?

(~~FOUO~~) My first thought for AOR is that a satellite in the 'Atlantic Ocean Region' is being discussed. For some people AOR will bring to mind the phrase 'Area of Responsibility.'

(~~FOUO~~) What about LOB? In some cases, LOB has an analytical meaning of 'Line of Bearing' for 'DF-ing' (Direction Finding) a signal. In other cases, LOB has a more managerial meaning of 'Lines of Business.'

(~~S~~) MEPP might make a typical _Tales of the KRYPT_ reader think about working with kids in elementary schools through the 'Mathematics Education Partnership Program.' For others, [redacted]

(~~FOUO~~) Now, what about the last acronym in this alphabetical listing - OTA? In DO, OTA typically refers to a signal that has gone 'Off the Air.' In DI, however, OTA refers to a signal which was transmitted 'Over the Air' (vice a signal that was generated in the lab). Slight difference? (b)(1) (b)(3)-P.L. 86-36

(~~FOUO~~) I have seen each of these acronyms used (under both of their (b)(3)-P.L. 86-36

[redacted]

meanings) in Agency documents without the acronyms being expanded. Of course, we are told that commonly known, standard acronyms ARE allowed to be used without expansion. But people seem to be unaware that 'standard' in one area of the Agency may not be 'standard' in another area of the Agency. So, I support the concept that ANY acronym which is to be used in a document MUST be expanded.

(U) And, what was the acronym which finally pushed me over the edge? Well, I'll leave that a mystery. But what acronyms annoy you?

~~(FOUO)~~ [redacted]

//

8.(U) EDITORIAL CORNER

REMINDER: (U) Submissions for the August issue are due by July 24.
PLEASE NOTE: (U) All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION-MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the editorial board.

(b)(3)-P.L. 86-36

~~(FOUO)~~ EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "DADR"
DATE OF SOURCE: 3 SEP 1991

[redacted]

(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

TOP SECRET//COMINT

(C) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:22
(U) PE EXTERNAL PAGE

****
* TALES OF THE KRYPT *
****
August 1998

//
****

++
//

(U) TABLE OF CONTENTS:

1. (U) Calendar of Events

2. (U) Cryptanalysis Career Panel (CACP) News

2a. (U) CACP Certification, Personnel Changes and New Interns

2b. (U) 1999 PQE Review Sessions

3. (TSC) KRYPTOS Society News: KRYPTOS Society Talk: [redacted] From Discovery to Exploitation, A Diagnosis Success Story" by [redacted] R51

4. (U) Community News

4a. (FOUO) GCHQ Names New Director (Information provided by [redacted] UKLO-2.)

4b. (FOUO) The Death of Frank Rowlett by David A. Hatch, Center for Cryptologic History [Article reprinted from the _Cryptologic Almanac_.]

5. (U) Technical Health

5a. (FOUO) Change Point Detection in Video Problems [redacted]

5b. (FOUO) "Creating Boolean Functions from Lookup Tables" (Summary of a talk presented by [redacted] [redacted] on 7 July, 1998.)

6. (FOUO) Puzzles by [redacted]

6a. (U) Answer to June-July Puzzle

6b. (U) August Puzzle

7. (U) Open Invitation to Apply for the Position of Puzzle Editor

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

8. (U) Editorial Corner

1. (U) CALENDAR OF EVENTS

(b)(1)
(b)(3)-P.L. 86-36

Sep 11 (U) CMP Graduation, Friedman Auditorium, 1300

Sep 15 ~~(TSC)~~ KRYPTOS Society Talk: [redacted] From Discovery to Exploitation, A Diagnosis Success Story" by [redacted]
R51
Friedman Auditorium, 1315 (Seating begins at 1300)
(See article 3.)

PLAN AHEAD

Oct 22 (U) Annual KRYPTOS Society Luncheon, Fort Meade Officers Club

Oct 26-29 ~~(C CCO)~~ CCWG Conference on Computer Communications:
C2C Target Development

(b)(3)-P.L. 86-36

Nov 2-6 (U) CONSCRYPT '98 at CSE

Nov 2-6 ~~(C)~~ Crypto-T/A Seminar, TA-310, OPS2B, 2B4118-6
(Formerly Annual CANUKUS Crypto-T/A Conference)

Dec 2 (U) A5 Reunion, Blob's Park

2. ~~(FOUO)~~ Cryptanalysis Career Panel (CACP) News by [redacted]
Assistant Executive, CACP

2a. (U) CACP Certification, Personnel Changes and New Interns

~~(FOUO)~~ Congratulations to [redacted] on her certification as a cryptanalyst!

~~(FOUO)~~ The CACP welcomes the following:

[redacted] as Member of the CA Technical Track Review Panel, and

(b)(3)-P.L. 86-36

[redacted] as Member of the CA Technical Paper Review Evaluation Board.

~~(FOUO)~~ The CA Intern Panel welcomes its newest interns, [redacted] hired by NSA in July; and [redacted] both hired in August.

2b. (U) 1999 PQE Review Sessions

(b)(3)-P.L. 86-36

[redacted]

~~(FOUO)~~ Study sessions for the 1999 CA PQE will begin in September on the following dates:

Thursday, 10 September, 0930-1100, OPS1, Room 3C082
Thursday, 24 September, 0930-1100, OPS1, Room 3C082

~~(FOUO)~~ Sessions will be held twice a month. The first session will focus on how the reviews will be run, topics that may be covered, and Playfair Squares, which seem to appear frequently on the PQE. Participants may also suggest particular topics for future sessions. If you would like to attend or want more information, please contact [redacted] (b)(3)-P.L. 86-36

//

3. ~~(TSC)~~ KRYPTOS Society News: KRYPTOS Society Talk: [redacted] "From Discovery to Exploitation, A Diagnosis Success Story" by [redacted] (b)(1) (b)(3)-P.L. 86-36

~~(TSC)~~ The KRYPTOS Society will sponsor a talk on September 15, 1998 at 1315 hours in the Friedman Auditorium. [redacted] will present "From Discovery to Exploitation, A Diagnosis Success Story."

[redacted] (b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

//

4. (U) COMMUNITY NEWS:

4a. ~~(FOUO)~~ GCHQ Names New Director
(Information provided by [redacted] UKLO-2.) (b)(3)-P.L. 86-36

(U) [N.B.: British spelling and usage have been preserved in this article.]

(U) GCHQ has announced that Mr. Francis Richards is the new Director, GCHQ.

(U) Mr. Francis Neville Richards (CMV, CVO), aged 52, was educated at Kings College Cambridge. He is married with 2 children, and his wife Gill is a radio and TV journalist.

(U) Mr Richards served in the Royal Green Jackets 1967-69. He joined the Foreign and Commonwealth Office in 1969, where he served in a number of posts at home and abroad (Russia, Austria and India) before becoming the UK's first High Commissioner in Windhoek, Namibia (1990-92) and was later Minister in Moscow (1992-95).

[redacted] (b)(3)-P.L. 86-36

(U) In January 1998, Mr. Richards was appointed Under Secretary, Defence & Intelligence as successor to Kevin Tebbit. Now Mr. Richards succeeds Mr. Tebbit yet again, this time as Director, GCHQ.

(b)(3)-P.L. 86-36

4b. ~~(FOUO)~~ The Death of Frank Rowlett
by David A. Hatch, Center for Cryptologic History
[Article reprinted from the _Cryptologic Almanac_.]

(U) The Center for Cryptologic History is sad to have to announce that Frank B. Rowlett passed away on June 29 at the age of 90. Mr. Rowlett was the last of William Friedman's original employees, hired for the Army's Signal Intelligence Service in 1930.

(U) Frank Rowlett was born on May 2, 1908, in Rose Hill, Virginia. He received a B.A. from Emory and Henry College with a major in mathematics and chemistry. He was hired by William Friedman as a "junior cryptanalyst" for the SIS on April Fool's Day in 1930; shortly thereafter he was followed in the SIS by Abraham Sinkov and Solomon Kullback.

(U) During the 1930s, Rowlett and his colleagues, after a lengthy period of training, worked as both cryptologists and cryptanalysts. They compiled codes and ciphers for use by the U.S. Army and began solving a number of foreign systems, notably Japanese. In the mid-1930s, Rowlett and his colleagues solved the first Japanese machine system for encipherment of diplomatic communications, known to the Americans as RED. From 1939 to 1940, Rowlett played a major role in solving a much more sophisticated Japanese diplomatic cipher machine, nicknamed PURPLE by the U.S. When asked what his greatest contribution to this effort was, Rowlett once said, "I was the one who believed it could be done."

(U) Friedman and Rowlett also had crucial roles in protecting American communications during World War II. Working with the U.S. Navy, they helped design the SIGABA, the cipher machine which was never solved by the Axis during the war. The security of this machine was also an important factor in saving American lives in combat. (In 1964, Congress awarded Rowlett $100,000 as partial compensation for his classified cryptologic inventions).

(U) In addition to having highly developed cryptanalytic skills, Rowlett was a good manager, and he rose quickly within the organization. From 1943 to 1945 he was chief of the General Cryptanalytic Branch, and from 1945 to 1947 he was chief of the Intelligence Division. From 1949 to 1952, he was technical director in the Office of Operations of the Armed Forces Security Agency, the predecessor to NSA.

(U) Rowlett differed with General Ralph Canine, the first director of NSA, over personnel movements, including his own. Acting on his differences, he transferred to the Central Intelligence Agency in 1952, and worked there until 1958. At that time he returned to NSA as a special assistant to the director. In 1965, Rowlett became Commandant of the National Cryptologic School. He retired from federal service in

(b)(3)-P.L. 86-36

1966.

(U) Because of his importance in the protection of American communications, the Information Systems Security Organization has named its highest award the Frank Byron Rowlett Award.

(~~FOUO~~) [David A. Hatch, Center for Cryptologic History, [redacted]

[redacted] (b)(3)-P.L. 86-36

5. (U) TECHNICAL HEALTH

[redacted]

[redacted] (b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

(~~FOUO~~) Work on this problem is continuing. [redacted] (b)(6) (b)(7)(C) OGA FBI integree, has written another paper on the subject. It is also being looked at by the Director's Summer Program participants and the NSA Statistical Advisory Group.

5b. (~~FOUO~~) "Creating Boolean Functions from Lookup Tables"
(Summary of a talk presented by [redacted] [redacted] on 7 July, 1998.)

[redacted] (b)(3)-P.L. 86-36

[redacted] (b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

6. ~~(FOUO)~~ PUZZLES
by [redacted] (b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36
(b)(6)

6a. ~~(FOUO)~~ June-July Puzzle - Vexing Vocabulary

[redacted]

(U) This is a puzzle combining elements of vocabulary and deductive reasoning. The object is to form a word in each row by placing one letter in the empty space in the middle column. Each letter of the alphabet must be used once and only once. Nearly all rows have more than one possible word that can be formed. For example, in the first row, the blank could be filled by a G, K, M, N, P, or V, giving the words OBLIGE, LIKED, MEDAL, LINED, PEDAL, or LIVED, respectively. All words must be formed with consecutive letters in the row (i.e., no skipping over letters), they must use the letter you put in the blank space (that letter can appear anywhere in the word), the word must be at least three letters long, and only standard, non-capitalized, non-foreign words are allowed (exceptions are allowed for British spellings :-)). Extra credit goes to anyone whose words are all at least five letters long - I don't have a solution for that, but it theoretically is possible.

1 OBLI_EDAL
2 PISC_REAL
3 NOVE_RUNK
4 AGEN_AGER
5 THIR_YALS
6 ADIN_USTO
7 TUXO_IOUS
8 OSTR_PEDE
9 OSTA_PINE
10 INCO_ERAS
11 APRE_TIGE
12 VALS_ACKS
13 SCAN_ONLE
14 INDA_GERT
15 FINE_ACTS
16 THER_ANTS
17 UPED_NTAL
18 CRAS_UEST
19 PRIN_LUXY
20 IMPO_ONER
21 GRAP_ICED
22 PENC_LORS
23 ALGE_RANT
24 PREL_DENT
25 OWAT_HARE

(b)(3)-P.L. 86-36

[redacted]

26 OBAC_LOGE

Solution:
(FOUO) There were probably as many solutions as solvers here. :-)
I have randomly picked out the following solution, with all words at least 5 letters long, from [redacted] The inserted letters appear in caps:

obliGed
cEreal
noveL
agenDa
thirTy
inCus
Pious
trIpe
staMp
coVer
preStige
Jacks
canYon
daNger
ineXact
erRant
pedAnt
Quest
inFlux
oZone
grapHic
cOlors
algeBra
prelUde
Whare
bacKlog

~~(FOUO)~~ Solutions were provided by: [redacted]

[redacted] (b)(3)-P.L. 86-36

6b. ~~(FOUO)~~ August Puzzle - Strange Bedfellows [redacted] (b)(3)-P.L. 86-36 (b)(6)

[redacted]

(U) In this puzzle, you are given a list of words, and you must find out what they have in common. For example, given the words TAPESTRIES, BARSTOOL, SEARED, SAGACITY, and MISTRUST, the answer is that each can be split in half to get two new words (TAPES and TRIES, etc.). As another example, given the words BALL, VENT, LUMPKIN, and CARROT, the answer is that if you replace the first letter by a P, you get another word.

[redacted] (b)(3)-P.L. 86-36

[redacted]

(U) Here are two lists of words to try:
1) BARF
BONKED
BOOMING
FINGER
HERO
JEALOUS
KIPPER
LAG
MANY
MILLION
RAP
TAXIS
TESTY
WED
WITHER
WIG
WOUNDS

2) PROLONG
DIALOUT (stretching things here - it should be dial out :-))
TERMINUS
BULLDOZE
HANDBALL
PLATINUM
SANDBARS
BOOTLESS
TAGALONG (and again here)
SUBLIMINAL

(FOUO) Send all solutions, as well as ideas for puzzle submissions, to [redacted]

//

7. (U) Open Invitation to Apply for the Position of Puzzle Editor (b)(3)-P.L. 86-36

(FOUO) The Puzzle section of _Tales of the KRYPT_ (TOTK) has always been both mentally stimulating and entertaining, as evidenced by the numerous regular solvers, ongoing feedback to the TOTK Editor, and the emphatic outcry of protest whenever there is any possibility that an issue of _Tales_ might be published without it. [redacted] has been providing the puzzles for several years, but now is looking for a well-deserved retirement from this duty.

(FOUO) If you would like to become the person behind the puzzles, write to the TOTK Editor at [redacted] sending a sample puzzle input if you have one already. If more than one person is interested and qualified, each would only have to provide puzzles every other month or so. If you enjoy solving our puzzles, please consider providing new ones.

//

8.(U) EDITORIAL CORNER

REMINDER: (U) Submissions for the next issue are due by 3 September.

PLEASE NOTE: (U) All submissions must be in ASCII format, and, with the

[redacted] (b)(3)-P.L. 86-36

implementation of E.O. 12958, MUST BE PORTION-MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the editorial board.

~~(FOUO)~~ EDITORIAL BOARD

[redacted] (b)(3)-P.L. 86-36

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

Return to Kryptos Home Page

NSA Home Page

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

[redacted]

(b)(3)-P.L. 86-36

[redacted]

~~TOP SECRET//COMINT~~

(S) POC: [redacted] info
(U) *Last Modified: 10/30/2002 11:42:24*
(U) PE EXTERNAL PAGE

~~TOP SECRET UMBRA~~

****
*** TALES OF THE KRYPT ***
****

September-October 1998

//
********** (b)(3)-P.L. 86-36

++
//

(U) TABLE OF CONTENTS:

1. (U) Calendar of Events

2. (~~FOUO~~) Cryptanalysis Career Panel (CACP) News
by [redacted] Assistant Executive, CACP

2a. (U) CACP Certification, Personnel Changes and New Interns

2b. (U) Technical Track Titling

3. (U) KRYPTOS Society News

3a. (~~FOUO~~) Winners Announced:
Peter Jenks Community Service Award - [redacted]
Norman Roberts Award - [redacted]

3b. (U) Annual Fall Luncheon

3c. (U) KRYPTOS Society Elections: 19 November 1998

3d. (U) Call for Volunteers to Produce KRYPTOS Society Video

4. (U) Community News

4a. (~~FOUO~~) Hugh F. Gingerich, in Remembrance [redacted]

4b. (U) Women in Mathematics Society (WiMS) Introduces "The WiMS Speakers Forum"

4c. (~~FOUO~~) Upcoming Crypto-T/A Seminar

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

by [redacted]

4d. (~~FOUO~~) Congratulations Class of 1998 Cryptologic Mathematician Program (CMP)
by [redacted]

4e. (~~FOUO~~) Extension of Nomination Deadline for the Sir Peter Marychurch Award.

5. (U) Technical Health

5a. (~~FOUO~~) Technical Track Conferences
by [redacted] CA Skill Field Director

5b. (~~FOUO~~) The SONET Ring Loading Problem
by [redacted]

6. (~~FOUO~~) Puzzles
by [redacted]

6a. (U) Answer to August Puzzle

6b. (U) September-October Puzzle

7. (U) Editorial Corner

(b)(3)-P.L. 86-36

"""""""

2. (~~FOUO~~) Cryptanalysis Career Panel (CACP) News by [redacted]
Assistant Executive, CACP

2a. (U) CACP Certification, Personnel Changes and New Interns

(~~FOUO~~) Congratulations to [redacted] on his certification as a cryptanalyst!

(~~FOUO~~) The CACP welcomes the following:

[redacted] as Members of the CA Career Panel, and [redacted] as Member of the CA Technical Track Review Panel.

(~~FOUO~~) The CA Intern Panel welcomes its newest interns, [redacted] who was hired in September and [redacted] who entered on duty at NSA this week.

(b)(3)-P.L. 86-36

2b. (U) Technical Track Titling

(~~FOUO~~) Congratulations to all recently titled members of the Cryptanalysis Technical Track.

MEMBERS

[redacted]

SENIOR MEMBERS

[redacted]

MASTERS

[redacted]

(b)(3)-P.L. 86-36

//

3. (U) KRYPTOS Society News

3a. (~~FOUO~~) Winners Announced:
Peter Jenks Community Service Award - [redacted]
Norman Roberts Award - [redacted]

[redacted]

(FOUO) The KRYPTOS Society is pleased to announce that the prestigious awards named in honor of Peter Jenks and in honor of Norman Roberts will be presented at the Society's annual luncheon to

(FOUO) The Peter Jenks Community Service Award, named for a celebrated Agency cryptanalyst, manager, and Career Panel leader, recognizes exceptional service to the Cryptanalytic Community. [redacted] was Chairman of the Cryptanalysis Career Panel during a critical time, providing wisdom, judgement, and counsel for many important decisions as cryptanalysis underwent transition into its current form.

(b)(3)-P.L. 86-36

(FOUO) The Norman Roberts Award acknowledges oustanding cryptanalytic contributions by junior (usually in their first five years of service) cryptanalysts. [redacted] has a string of impressive technical accomplishments which speak to his cryptomathematical prowess and remarkable versatility. Norman Roberts was a prominent British cryptanalyst, known for both innovative cryptanalytic techniques and inspired guidance of younger analysts, who died in a boating accident in 1990.

(FOUO) The awards will be presented at the Society's annual luncheon, held at the Fort Meade Officers' Club 22 October. At that time, seven new Distinguished Members, all recently retired, will also be recognized: [redacted]

(b)(3)-P.L. 86-36

(U) Panels of judges have also selected winners in the Society's annual recognitions of authors and speakers. The essay contest has been extant for many years, but the awarding of prizes for excellent talks on cryptanalytic topics is new this year. Winners have been notified, but their names will not be announced until the luncheon.

3b. (U) Annual Fall Luncheon

(U) The KRYPTOS Society Annual Fall Luncheon will be held on Thursday, 22 October 1998 at the Ft. Meade Officers' Club. The program will include the presentation and recognition of Distinguished Members, and the presentations of the Peter Jenks Community Service Award, and the Norman Roberts Award and the authors and speakers awards.

3c. (U) KRYPTOS Society Elections: 19 November, 1998

(FOUO) The KRYPTOS Society will be holding elections on November 19. The Election Committee would like to present the following slate of candidates.

PRESIDENT-ELECT:

SECRETARY:

[redacted]

(b)(3)-P.L. 86-36

[redacted]

MEMBER-AT-LARGE: [redacted]

3d. (U) Call for Volunteers to Produce KRYPTOS Society Video

(FOUO) If you are interested in working on the KRYPTOS Society's new video project, please contact [redacted] This is a unique and interesting opportunity to do a video from scratch--theme, planning, design, drafting text, interviews, working with the NSA TV Studio, etc. If you have always wanted to do something like this and would like to portray Cryptanalysis and the Cryptanalytic Community to a large audience, here's your chance. Videotaping interviews with recent retirees will definitely be a part of this project. Call [redacted] now!

(b)(3)-P.L. 86-36

"""""""

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TSC)~~ In the 1960's Dr. Gingerich designed a [redacted]

[redacted]

(U) Dr. Gingerich was born October 14, 1916, in Ann Arbor, the son of Solomon Gingerich, a professor of English literature at the University of Michigan, and Beulah Pearl Kauffman Gingerich. A brother, Horace Richard, who was five years older, died in 1927 of typhoid fever. After the family moved to Springdale, Arkansas, Hugh earned a bachelor's degree at the University of Arkansas in 1937 and a PhD at the University of Illinois in 1942, both in mathematics. His thesis, ``Generalized fields and Desargues configurations,'' has attained the status of a seminal work. (In about 1990, a young visiting professor named Ken Smith, while giving a lecture in R51, referred to ``Gingerich's Theorem,'' while unknown to him this same Gingerich sat in the next room.)

(U) After finishing his degree, Hugh taught at the University of Maryland, suffering under a football coach turned university president. In 1944 he moved to the Department of Terrestrial Magnetism at the Carnegie Institute of Washington. In 1946 he joined CSAW, an NSA predecessor, at the Naval Annex at Ward Circle in Washington, D.C. He remained at NSA until he retired in 1992.

~~(FOUO)~~ Dr. Gingerich was one of four math PhDs of his vintage from the University of Illinois. The others were Joseph Eachus, Richard Leibler, and Louis Tordella. The latter three were all naval officers and had all completed their Illinois degrees in 1939. Eachus and Tordella were already at CSAW prior to 1946, and in fact Eachus was instrumental in bringing Hugh in. When Eachus told Admiral Joseph Wenger (Director) that he would vouch for Hugh, Wenger accepted Hugh without the usual background investigation. (Leibler came in 1949, having earlier been on an aircraft carrier, in such environs as Iwo Jima.)

(U) It would be hard to pretend Hugh was without eccentricities. In the 1950's he often worked in a phone booth, so as not to be disturbed. In the 1960's his desk was stacked with boxes of cherry cordials, which would provide his lunch. After thoughtful research, he found he liked the cheaper ones best. In the late 1940's, he decided that the 24-hour day did not suit him. So he adopted a 28-hour day. In accordance with his six-day week, some days he'd be getting up in the middle of the night, or at dusk, or whatever. A nearby all-night Hot Shoppes restaurant helped make this work. But then he met Shirley, and it was back to 24-hour days.

(b)(3)-P.L. 86-36

[redacted]

(FOUO) Hugh met Shirley Smith in 1950, when she was translating Portuguese at the Agency. Within only a few weeks they were married. Shirley, who survives him and lives in Kensington, originally came from Brooklyn. The couple were avid bird watchers and pet enthusiasts. Hugh was a Redskins fan, and Shirley is an artist.

(FOUO) Of Amish ancestry, Dr. Gingerich wrote Amish and Amish Mennonite Genealogies with Rachel Kreider. It was published in 1986 by Pequea, of Gordonville, Pa. Besides Shirley, Hugh's only survivors are cousins in the Iowa Mennonite community.

(U) In appearance, Hugh was bearded, tall, slender, and knock-kneed. His power of concentration made him appear set-apart and somewhat rough-hewn. He'd be at his desk, and yes, he'd be smoking. But he'd once in a while get up and come to you. He'd often have some sort of a genealogical puzzle, which he'd represent as an exercise in cryptanalysis. He'd eventually invite you to his house, where you'd meet his energetic and charming wife, and his many cats and dogs. There were also several skunks, including Desert Flower, who had the run of the house, and would pull things out of kitchen cabinets. You would come to know a Hugh who was gentlemanly, proper, sophisticated, and proud. But he was also lively and boyish, and could be a rascal. He could turn a phrase to the very end of his life. Those of us who programmed for him, or worked near him, will miss this kindly man.

4b. (U) Women in Mathematics Symposium (WiMS) Introduces "The WiMS Speakers Forum"

(U) The Women in Mathematics Symposium (WiMS) has conceived a forum out of a desire to foster a sense of community among the professional women mathematicians at the NSA.

(U) The speakers' forum will be comprised of a series of presentations designed to enhance career development in several ways. Firstly, invited speakers will be asked to address issues that are relevant to our career opportunities and to enhancing the effectiveness of women in the workplace. Secondly, by providing an opportunity for interaction among women mathematicians at all career stages throughout the Agency, the benefits of mentoring and networking can be realized without formally setting up any structured mentor-mentee relationships.

(FOUO) The first invited speaker will be [redacted] Her talk is entitled:

"Catch Yourself Doing Something Right:
Striving for Excellence vs. Perfection"

(b) (6)

(FOUO) [redacted] gave a similar talk at the NSA last year as part of the Women's Equality Day, sponsored by the Federal Women's Program, and it was very well-received. WiMS has invited her back again as part of this Forum, and has asked her to gear her talk to the members of our technical community, who may have missed her previous presentation.

(U) The Speakers' Forum will be held on:
October 29, 1998

(b) (3)-P.L. 86-36

[redacted]

1300-1500
in the Canine Suite.
Discussion and refreshments will follow.

(FOUO) Attendance is free, but limited. If you would like to attend, please obtain a ticket from one of the following:

[redacted]

(b)(3)-P.L. 86-36

(FOUO) If you prefer, you may also e-mail to [redacted] and request that a ticket be sent to you through Agency mail.

4c. (FOUO) Attendees to Modified Annual CANUKUS Crypto-T/A Conference to Receive NCS Course Credit; Call for Talks Issued by [redacted] M3 Technical Director for Crypto-T/A

(FOUO) What has been known as the annual CANUKUS Crypto-T/A Conference will be conducted as a seminar this year under course designator TA-310. Emphasis will be on both the crypto-T/A techniques employed and the intelligence gained to facilitate analysts applying similar techniques to a variety of targets. The seminar will now also be open to all Second Party partners dependent upon the classification of individual presentations.

(FOUO) This is the first year that NCS credit will be available for attendees to these presentations. NCS credit was sought to benefit the attendees in pursuit of maintaining technical track status, but a follow-on benefit is that the speakers will profit in a similar fashion. Other designators, such as TD or CA, were investigated before the TA-310 designator was assigned. TA-310 is an existing designator for seminars covering SRTD-related topics.

(U) After the course designator was assigned, a call for talks and speakers was distributed across NSA, to GCHQ, CSE and field sites. Two topics from GCHQ, one from C Group, four from M, one from R and three from Z were initially identified. The final schedule of talks was issued in mid-September with the presentations to be given the first week of November in room 2B4118-6.

4d. (FOUO) Congratulations Class of 1998 Cryptologic Mathematician Program (CMP)
by [redacted] Z713

(b)(3)-P.L. 86-36

(FOUO) On 11 September 1998, in the Friedman Auditorium, the 33rd class of the Cryptologic Mathematician Program (CMP) graduated. The Master of Ceremonies was [redacted] Executive, Cryptologic Mathematician Program. The opening remarks were made by [redacted] Chief, Techniques and Research. Mr. James R. Taylor, Deputy Director for Operations gave the keynote address. Various members of

[redacted]

the NSA mathematics community attended the event, along with other Agency personnel, family members and friends.

(U) During their three-year program, class members attended many training classes, conferences and went on a variety of class trips.

(U) Some of the class members' accomplishments included: [redacted] promotions, [redacted] cash awards, and [redacted] letters of appreciation.

~~(FOUO)~~ Following is the list of graduates and their first assignment after graduation: (b)(3)-P.L. 86-36

[redacted]

(U) CONGRATULATIONS TO ALL!

4e. (U) Extension of Nomination Deadline for the Sir Peter Marychurch Award

~~(FOUO)~~ Nominations are due for the Sir Peter Marychurch Award established in 1989 by NSA and GCHQ to recognize significant cryptanalytic achievement by either an NSA or GCHQ cryptanalyst, cryptomathematician, or group of cryptanalysts and/or mathematicians. Submissions for cryptanalytic work performed during the period of 1 July 1997 through 30 June 1998 are due to Chief, Z07 by 2 November 1998.

//

5. (U) TECHNICAL HEALTH

5a. ~~(FOUO)~~ Technical Track Conferences by [redacted] CA Skill Field Director (b)(3)-P.L. 86-36

~~(FOUO)~~ You may know that the Cryptanalysis Technical Track has a budget, through the DO Technical Health Advisory Board (THAB), to send technical track members to conferences which will improve their technical skills and knowledge. Up until now, the procedure was that individuals would submit a request to the SFD when they learned of a conference that they wanted to attend. Beginning in FY-99, we are taking a more proactive approach by having a group of techies decide in advance which conferences would be beneficial to attend, and how many people should go. A committee was formed of technical track members to help the CA Skill Field Director (SFD) plan for technical conferences for the upcoming fiscal year. These conferences will be advertised throughout the year to technical track members, who may submit an application to attend with THAB funding.

(U) Below is the list of conferences that the committee has (b)(3)-P.L. 86-36

[redacted]

selected for attendance. People have already been selected to attend the Microsoft Developers Conference, WCRE (Reverse Engineering), and CONSCRYPT this year. Watch the DO THAB home page for reports on these conferences, as well as others from last year. (Trip reports are currently on the WEB for the 1998 RSA Data Security Conference, International Cryptologic Common Data Format Working Group, and Personal Indoor and Mobile Radio Communications Conference.)

(~~FOUO~~) If you think one of these conferences would be particularly beneficial to your technical development and would like to attend, please fill out the application located on the DO THAB conference program WEB page: [redacted]

The conference committee will select the most appropriate person to attend from all applications received. Since only one person will be funded for each conference, the selectee will be required to write a trip report, make available to others all materials received at the conference, and perhaps even give a technical talk or workshop on what was learned, if there is interest. You are also welcome to submit applications for conferences which are not on the list below, if they will enhance your CA skills. Please have your conference application in by the due date listed, and contact [redacted] if you have any questions about the procedures. (b)(3)-P.L. 86-36

(U) Note: you must be a member of the CA Tech Track to apply for funding.

[redacted]
CA Skill Field Director

(U) CONFERENCE	DATES	DUE DATE
SANS Network Security	24-31 Oct.	immediately
5th ACM Conference on Computer and Communications Security	2-5 Nov.	23 Oct.
WebNet '98	7-12 Nov.	23 Oct.
RSA Data Security	17-21 Jan.	31 Dec.
FSE 99 (Fast Software Encryption)	24-26 Mar.	26 Feb.
Eurocrypt 99	2-6 May	2 Apr.
SUPERCOM '99	6-10 June	7 May
Crypto 99	summer 99 - TBA	7 May

5b. (~~FOUO~~) The SONET Ring Loading Problem
by [redacted] Z21 (b)(3)-P.L. 86-36

(U) The increasing use of fiber optic technology to provide high-bandwidth communications services has led to the appearance of

[redacted]

large-scale synchronous optical networks using a ring topology (SONET rings). A SONET ring may be described as a network of n nodes, numbered from 0 to n-1 starting at the top of the ring and proceeding clockwise, connected to a circular fiber optic cable. To configure the network, a separate channel of a specified bandwidth along the ring connects each pair of nodes. The ring is bidirectional; a channel connecting nodes a and b (say), may be considered to carry all traffic from a to b as well as from b to a. A channel (a,b) is said to be routed clockwise if a < b, and counterclockwise if b < a. For example, the traffic between nodes 3 and 6 will either pass (clockwise) through nodes 4 and 5 or (counterclockwise) through nodes 2,1,...,8,7.

(U) The task of configuring the network is precisely the task of choosing one of two directions for each pair of nodes. For a given configuration, the total required bandwidth for the kth link, (defined as the path between nodes k and k+1), may be computed as the sum of all channels passing through nodes k and k+1 in the clockwise direction and nodes k+1 and k in the counterclockwise direction. Although the fiber optic cable may be considered to provide unlimited bandwidth, hardware costs, (in particular, expensive add/drop multiplexers), and the possibility of traffic loss from link failures make it desirable to find the network configuration that minimizes the maximum demand on any link. This is the SONET Ring Loading Problem.

(U) Although the SONET Ring Loading Problem has been demonstrated to be at least as hard as the NP-complete PARTITION problem, recent work by Cosares and Saniee (1994), Schrijver, Seymour, and Winkler (1997), and Khanna (1997), has provided the theoretical and practical basis for efficient deterministic algorithms that produce near-optimal routings. For our study, we implemented the algorithm due to Schrijver, Seymour, and Winkler and compared its performance to that of several algorithms based on randomized local search--specifically, Tabu Search, the Metropolis Filter, Simulated Annealing. We also describe a new algorithm called Direct Discrete Descent (DDD). For problems with large variance among the pairwise traffic demands, the DDD algorithm typically obtains better ring configurations than the others, although at greater computational cost than the algorithm of Schrijver, Seymour, and Winkler. All of the algorithms were programmed in the C programming language and run under Linux on a 166 MHz Pentium Dell laptop.

"""""""

CARROT, the answer is that if you replace the first letter by a P, you get another word.

(U) Here are two lists of words to try:

1) BARF
BONKED
BOOMING
FINGER
HERO
JEALOUS
KIPPER
LAG
MANY
MILLION
RAP
TAXIS
TESTY
WED
WITHER
WIG
WOUNDS

2) PROLONG
DIALOUT (stretching things here - it should be dial out :-))
TERMINUS
BULLDOZE
HANDBALL
PLATINUM
SANDBARS
BOOTLESS
TAGALONG (and again here)
SUBLIMINAL

(U) Solution: In the first list, you can replace the first letter of each word by a 'Z' to get a new word. In the second list, replace the last two letters of each word with a 'G' to get a new word.

(U) Solutions were provided by: [redacted]

6b. (U) September-October Puzzle - Say What? [redacted] (b)(3)-P.L. 86-36

(U) Following are a number of series of words that look like gibberish, but if pronounced correctly, sound like a meaningful phrase. An example of this is the code signature used by one of the U.S. Presidents. He wrote: Ale In Can, which when pronounced in a slightly twisted way, reveals A. Lincoln. Have a go at these. Because they're a little odd, a category is provided to help guide your search. (b)(3)-P.L. 86-36 (b)(6)

Category	Words to Decode
Physics Phenomena	Arm, moniker, moe, shun
Book Title	Bate, Riyadh, gay, aims

(b)(3)-P.L. 86-36

[redacted]

Physics Formula	Effie, quill, Sam, May
Physics Concept	Eyes, umber, guns, ardent, deep, rinse, sable
Disney Saying	Hack, unum, mitt, ta-da
Shakesperean Play Quote	Hoe, why, yams, lain
Book Title, in French	Lipid, deep, rants
Shakesperean Character	Omelette, print, soft, tan, mock
World Leader	Poe, budge, on, ball, thus, sack, end
Literature Title	Thud, eh, though, fee, Vanilli, itch
Musical Title	Vent, a, muff, tee, up, bra
Cartoon Characters	Yak, cow, walk, owe, went, tot

(~~FOUO~~) Send all solutions, as well as ideas for puzzle submissions, to [redacted]

7.(U) EDITORIAL CORNER (b)(3)-P.L. 86-36

REMINDER: (U) Submissions for the next issue are due by 28 October.

PLEASE NOTE: (U) All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION-MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the editorial board.

(~~FOUO~~) EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted] (b)(3)-P.L. 86-36

~~TOP SECRET UMBRA~~

Derived from: Multiple Sources
24 February, 1998
Declassify on X1, X3, X5, X6, X7, X8

DERIVED FROM: NSA/CSSM 123-2
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

~~TOP SECRET UMBRA~~

[redacted]

9/24/2010

~~TOP SECRET UMBRA~~

~~(C)~~ *POC:* [redacted] *info*
(U) *Last Modified: 10/30/2002 11:42:23*
(U) PE EXTERNAL PAGE

~~TOP SECRET UMBRA~~

TALES OF THE KRYPT
November-December 1998

(U) TABLE OF CONTENTS:

1. (U) Calendar of Events

2. ~~(FOUO)~~ Cryptanalysis Career Panel (CACP) Personnel Changes by [redacted], Assistant Executive, CACP

3. (U) KRYPTOS Society News

3a. (U) KRYPTOS Society Election Results

3b. ~~(FOUO)~~ 1998 Inductees as KRYPTOS Society Distinguished Members: [redacted]

3c. ~~(FOUO)~~ [redacted] Wins Peter Jenks Community Service Award

3d. ~~(FOUO)~~ [redacted] Wins Norman Roberts Award

3e. ~~(FOUO)~~ Results of First Annual Technical Talk Competition: Remarks by 1997 President Elect, [redacted] at the 1998 KRYPTOS Society Luncheon

3f. (U) Winners of 1998 KRYPTOS Literature Award

3g. (U) Call for Volunteers to Produce KRYPTOS Society Video

3h. (U) Breakfast Affair for Newly Certified Cryptanalysts

4. (U) Community News

4a. ~~(FOUO)~~ Reprint of _CRYPTOLOGIC ALMANAC_ article: Ernst Fetterlein (?1868-1944?)--For Tsar and King, Cryptanalyst Extraordinaire by [redacted]

4b. (U) Women in Mathematics Symposium (WiMS) Calls for Volunteers

4c. ~~(FOUO)~~ Greetings from Cheltenham Chapter by [redacted]

4d. ~~(FOUO)~~ The Operations Research Career Panel Presents the January 1999 Technical Social: "Confidence Scoring in Speech Recognition: Logistic Regression at NSA"

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

by [redacted]

5. (U) Technical Health

5a. (FOUO) Chromosome Classification by [redacted] IDA/CCS, [redacted] University of Maryland, College Park, and [redacted] Oak Ridge National Laboratory

5b. (FOUO) Summary of Recent [redacted] Developments by [redacted] Z233

5c. (U) Technical Reference Guides

6. (FOUO) Puzzles by [redacted] Z841

6a. (U) Answer to September-October Puzzle

6b. (U) November-December Puzzle - Annual "KRYPTOS KRISTMAS KWIZ"

7. (U) Editorial Corner

---

1. (U) CALENDAR OF EVENTS

Jan 6 (FOUO) Signals Analysis Association presents [redacted] "Extracting Text from Color Images", 0915, Friedman Auditorium

Jan 7 (U) Operations Research Career Panel January 1999 Technical Social 1300-1430 D5 Conference Room, OPS2B, Room 2B4118-2

Jan 26 (U) BANCC (Breakfast Affair for Newly Certified Cryptanalysts), 0800-1000

(U) PLAN AHEAD

May 17-21 (U) 1999 Signals Analysis and Development Conference

---

2. (FOUO) Cryptanalysis Career Panel (CACP) Personnel Changes by [redacted] Assistant Executive, CACP

(FOUO) The CACP welcomes:

[redacted] DO Skill Field Representative, as Member of the CACP,
[redacted] as Member of the CA Technical Track Review Panel, and
[redacted] as Member of the CA Technical Paper Evaluation Board.

[redacted]

3. (U) KRYPTOS Society News

3a. (U) KRYPTOS Society Election Results

(~~FOUO~~) The KRYPTOS Society is pleased to announce the winners of the 1998 Election.

The newly elected officers are:

[redacted] President-Elect

Secretary

Member-at-large

Member-at-large (b)(3)-P.L. 86-36

3b. (~~FOUO~~) 1998 Inductees as KRYPTOS Society Distinguished Members:

[redacted]

Remarks at the 1998 KRYPTOS Society Luncheon, by KRYPTOS Society President [redacted]

(U) Good afternoon, ladies and gentlemen, and welcome to the awards section of the annual KRYPTOS Society luncheon.

(~~FOUO~~) It is our special pleasure to recognize two sets of guests: those who are attending their first KRYPTOS Society luncheon and those Distinguished Members of the Society who are present. Our schedule is so busy that we won't be able to say anything individually about the returning Distinguished Members, but no doubt you've already heard other cryppies reminisce about their accomplishments. I'll try to do this alphabetically: [redacted]

(U) Next, I'd like to invite all those who are attending their first KRYPTOS Society luncheon to stand. These new arrivals into our Community represent our future. They are few in number but impressive in qualifications. When your hiring allocation is minimal, you can afford to choose only the best, and we have. I hope all of us will make welcome those who are ensuring the continuing tradition of excellence in our government's cryptanalytic service. Thank you for coming, and we hope to see you at future KRYPTOS Society luncheons as we celebrate together the responsibilities we have shared.

(b)(3)-P.L. 86-36

(~~FOUO~~) Next we'd like to recognize current Society members who have worked very hard to make possible what we do here. The luncheon itself has been planned and organized by [redacted] and her excellent team: [redacted] The judges for the essay contest were [redacted] The judges for the tech talk contest were [redacted] organized the contest. [redacted] performs our liaison with the retired members. I am [redacted] the current President of the Society, and I'd like to introduce our President-Elect, [redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted], who will be sharing with me the privilege of introducing our new Distinguished Members. A very brief citation, limited to an unclassified distillation of many years of classified achievement, will be read, and the new Distinguished Members will be invited to say a few words to their colleagues.

(b)(3)-P.L. 86-36

(U) Distinguished Membership in the KRYPTOS Society is conferred on those very few cryptanalysts whose contribution to the Community is so great that many can stand on their shoulders. There is no single route to attaining this recognition. It is our way of saying "thank you" for a lifetime of effort which has substantially advanced the prospects of the younger people to whom the torch has now been passed. Today it is our privilege to honor seven gentlemen whose long and illustrious careers have surpassed the criteria established for greatness in our profession.

(U) Our first two honorees share not only their careers but also their origins. Both hail from the state of Maine. That seems a remarkable coincidence, but it's a distinguishing characteristic which I share with them. You're unlikely to know many folks from Maine, since most of us prefer to stay pretty close to home, but a few of us have sought our fortunes in, as Downeasterners say, the southwestern 49.

(b)(3)-P.L. 86-36

(FOUO) [redacted]

(FOUO) There's another remarkable coincidence which, so far as we know, makes our first honoree, [redacted] unique. [redacted]

[redacted]

(FOUO) [redacted]

(b)(6)

[redacted]

(FOUO) For the major, significant, and long-range contributions [redacted] made to the mission of this Agency, he was awarded the Meritorious Civilian Service Award in 1983.

(FOUO) For his service and performance as Chief of the Z Group Specified Special Programs Staff, [redacted] received the Exceptional Civilian Service Award in 1993.

(b)(3)-P.L. 86-36

[redacted]

(FOUO) [redacted] (b)(3)-P.L. 86-36

[redacted] (b)(3)-P.L. 86-36 (b)(6)

Subsequently he worked in P12 and G492, then became Chief of G434. Following an integrated tour at GCHQ, [redacted] served as Deputy Chief of G43; Chief of the [redacted] project; Deputy Chief, A53; Chief of R21; Chief, Z4; and Deputy Chief, Q4. Ed served as President of KRYPTOS, 1991-1993.

(FOUO) During his career at the National Security Agency, [redacted] made many significant contributions in the field of cryptanalysis. He spent a significant portion of his career specializing in the cryptanalysis of signals. His early career was devoted to the development at the Agency of an ability to handle signals: in cryptanalysis, in reverse engineering, in data forwarding, and in signals processing. [redacted] foresaw the coming importance of signals analysis, and helped to establish Signals Analysis as a primary component of Cryptanalysis. (b)(3)-P.L. 86-36

(FOUO) [redacted] directed the efforts of a major cryptanalytic division working on a very diverse set of programs which included cryptanalysis of signals, computer systems and engineering support, as well as a special program. He was involved in projects to initiate three different overseas operations under the aegis of another agency. While serving as Chief of Z4, he completely reorganized the office. He recognized that we were facing unprecedented changes in our targets and the technologies they use, and began the work on a strategic plan to focus efforts on the challenges of the future.

(FOUO) [redacted] (b)(3)-P.L. 86-36 (b)(6)

(FOUO) [redacted]

After five years with MCC (Bobby Inman's supercomputer consortium) in Austin, TX, [redacted] rejoined IDA-CCR in LaJolla, and has only recently settled into a quasi-retired status. [redacted] can still be found teaching courses in one of his several specialties at the National Cryptologic School.

(FOUO) [redacted] has an enormous reputation as both a researcher and an expositor, and has been involved in many operational successes as well. [redacted] has pioneered several successful cryptanalytic techniques, from conception, through research and development, and into production. [redacted] is also well known for his collaboration with many of our other best minds. His breadth of knowledge, penchant for simplification, and clarity of exposition have led to his papers being widely read and understood. There are few important cryptomathematical problems to which [redacted] has not contributed insight or algorithm. (b)(3)-P.L. 86-36

[redacted]

(FOUO) [redacted]

[redacted]

(FOUO) [redacted] was one of the founding fathers, and certainly the chief guru, of Crypto-T/A. Many of us have fond memories of [redacted] poring over a diary, eyes close to the page, teasing the last bit of information from an event in the data.

(FOUO) He loved explaining what he and other analysts had discovered. And it didn't matter whether the analysis had been done that morning or 40 years ago, [redacted] knew it all personally!

(FOUO) [redacted] made many friends across the community and was proud to have played a modest part in maintaining and developing these relationships. In recognition of his remarkable achievements, [redacted] received a Distinguished Service Award from the Director of GCHQ shortly before he retired.

(b)(3)-P.L. 86-36

(FOUO) [redacted]

(FOUO) [redacted]

(b)(3)-P.L. 86-36
(b)(6)

[redacted] After four years in Operations, [redacted] enjoyed a tour in England as an integree, 1976-1979. [redacted] served as Chief, R21; Chief, G42; Chief, Z2, and finally Deputy Chief, then Chief, of Z, 1995-1997.

[redacted]

(FOUO) As Deputy Chief of Z, [redacted] led a group of senior Agency personnel in a strategic planning process which ultimately became the National Cryptologic Strategy for the twenty-first century. [redacted] then went on to become Chief of Z, recognized as being the most technically competent work force at NSA. He articulated the vision for the organization, encouraged workers to think "outside the box", created an environment that met current intelligence needs, and freed many of NSA's best and brightest to prepare for future technological challenges. The success of the Cryptanalysis Group in years to come will owe much both to [redacted] personal technical accomplishments and to his leadership of the men and women who carry out the Agency's cryptanalytic mission.

(b)(3)-P.L. 86-36

(FOUO) [redacted]

[redacted]

[redacted]

(~~FOUO~~) The foundation of [redacted] career was his deep love and mastery of languages, particularly his ability to master obscure languages >from little more than a grammar and a dictionary. This linguistic ability, coupled with first-rate cryptanalytic skills, made [redacted] a formidable practitioner of manual cryptanalysis.

(~~FOUO~~) One highlight of [redacted] career was his work on VENONA, with one particularly difficult and important text being styled "the [redacted] translation" in the official history.

(b)(3)-P.L. 86-36
(b)(6)

(~~FOUO~~) [redacted] dedication, tenacity, patience and enthusiasm in the face of difficult problems were outstanding. His willingness to share and pass on his knowledge and experience by working closely with less experienced staff has been a major factor in GCHQ's ability to maintain a high level of capability in manual cryptanalysis.

(b)(3)-P.L. 86-36

(~~FOUO~~) [redacted]

(b)(3)-P.L. 86-36

(~~FOUO~~) [redacted]

[redacted]

on 18 Oct 1965 as a Cryptanalysis Intern.

(~~FOUO~~) [redacted] quickly found recognition as a stellar cryptanalyst, and remained one throughout his career, but much of his fame is due to his eminence as a teacher, a rare combination of skills. As an instructor at the National Cryptologic School (1980-1987), he developed and taught courses both at home and abroad, and was a "Teacher of the Year" Finalist in 1985. [redacted] developed a new course for SPICE 1986 entitled Creative Cryptanalytic Thinking and was named Adjunct Faculty teacher of the year.

(~~FOUO~~) [redacted] mastery of the cryptanalytic arts has brought him into some problems which can only be termed bizarre, even by Agency standards, and he has used some equally bizarre methods to solve them. At the end of his career, [redacted] organized and captained a powerful interorganizational team to deal with unusual and difficult problems which had defied solution. One of his goals was to bring junior analysts into intimate contact with the thinking of more experienced analysts. His true legacy to the CA Community lies in the countless analysts who carry on their cryptanalytic pursuits using the diagnostic skills and cryptanalytic techniques they learned from him.

(b)(3)-P.L. 86-36

3c. (~~FOUO~~) [redacted] Wins Peter Jenks Community Service Award

[redacted]

(~~FOUO~~) The Peter Jenks Community Service Award, jointly sponsored by the Cryptanalysis Career Panel and the KRYPTOS Society, recognizes exceptional service to the Cryptanalytic Community. Peter Jenks, a celebrated Agency cryptanalyst, manager, and Career Panel leader, was a powerful promoter both of cryptanalytic excellence and of suitable rewards for cryptanalytic achievement.

(~~FOUO~~) The Cryptanalysis Career Panel and the KRYPTOS Society are pleased to announce that [redacted] has been selected to receive this award. As Chairman of the Cryptanalysis Career Panel at a critical time, [redacted] provided wisdom, judgement, and counsel for many important decisions as cryptanalysis underwent transition into its current form.

(~~FOUO~~) [redacted] has served the Cryptanalytic Community in many ways. He has been president of KRYPTOS. He has been Deputy Chief of Z4. He has initiated many efforts to secure increased recognition for cryptanalytic achievement and to promote harmony and constructive interaction within the Community. Most recently, [redacted] has served as a dynamic Chairman of the Cryptanalysis Career Panel.

(b)(3)-P.L. 86-36

(U) It is easy for all of us to overlook the functioning of the Career Panel. When its job is done right, its objectives accomplished, the result is that we are unaware that any problem ever existed. But the Career Panel determines the direction of Cryptanalysis: by establishing the requirements for professionalization, by deciding which courses are important, which offices deserve intern support, and what skills are necessary to merit being called a Cryptanalyst.

(~~FOUO~~) All of us know that Cryptanalysis has been in crisis for the last few years. These are transitional times, when our very existence as a profession has been called into question. Traditional applications have given way to modern ways at a rapid pace. Those who fail to adapt have been swept away. Fortunately for us, the ship of Cryptanalysis has been guided through these turbulent waters by our intrepid helmsman, [redacted]

(~~FOUO~~) Under [redacted] leadership, the Panel has completely revised its requirements and policies. For the benefit of our retired members, I can say that Cryptanalysis remains well and healthy. But the classical concept of cryptanalysis which you nurtured is gone forever. Today's cryptanalyst still solves difficult problems for which no textbook has been written. That's what you did; that's what cryptanalysts will always do. But the problems themselves have changed decisively and success requires a much different preparation.

(~~FOUO~~) Cryptanalysts have always been known for their breadth: many of us are proudly multi-disciplined. Tech track innovations have forced the Agency's technical work force to choose among ten disciplines, nine of which are very narrow and one which is dangerously broad. The members of that one Career Panel travel a difficult road, trying, on the one hand, to provide career opportunities and recognition for individuals who are contributing to the Agency mission, but who fall outside the nine narrow career paths and, on the other, to adequately prepare cryptanalysts to solve the difficult problems of the future. [redacted] and his colleagues have succeeded admirably, but it has required many, many hours of work and

(b)(3)-P.L. 86-36

[redacted]

painfully careful deliberation. This is our chance to thank [redacted] for his leadership. He's had a good team, it's true, but ultimately his ideas have been the key to success. The cryptanalysts of the future owe a huge debt to [redacted]

3d. (~~FOUO~~) [redacted] Wins Norman Roberts Award

(~~FOUO~~) The Norman Roberts Award acknowledges outstanding cryptanalytic contributions by junior (usually in their first five years of service) cryptanalysts. [redacted] has a string of impressive technical accomplishments which speak to his cryptomathematical prowess and remarkable versatility. Norman Roberts was a prominent British cryptanalyst, known for both innovative cryptanalytic techniques and inspired guidance of younger analysts, who died in a boating accident in 1990.

(~~FOUO~~) Norman Roberts was a fine cryptanalyst and teacher. I had the pleasure to know Norman when I was integrated into GCHQ: a gentleman, always willing to listen to your ideas, always eager to improve his own. Norman was highly prized as a colleague, both for his brilliance and for his seeming interest in every problem.

(~~FOUO~~) The award which bears his name is intended to reward similar skills in others, and this year we recognize that same spirit, intellect, and character in the person of [redacted] has recently completed the Cryptologic Mathematician Program with distinction, having made a substantial technical contribution in each of the offices in which he toured.

(~~FOUO~~) That achievement alone is not enough to make [redacted] unique. Indeed, we are blessed with many extremely able young cryptomathematicians who have achieved much and who will continue to achieve much. What sets [redacted] apart is his ability to draw the best >from others, that same quality which set Norman Roberts apart from his peers. Many of [redacted] colleagues have commented on the benefits of discussing their problems with [redacted] Cryptanalysis is a difficult business. Almost no important problems are solved by individuals working alone. We need brilliance, and we also need team players. Today we're recognizing both of those traits in one person: [redacted]

(b)(3)-P.L. 86-36

3e. (~~FOUO~~) Results of First Annual Technical Talk Competition; Remarks by 1997 President Elect, [redacted] at the 1998 KRYPTOS Society Luncheon

(b)(3)-P.L. 86-36

(U) The first annual Technical Talk competition sought to recognize the best technical presentation on a subject relating to cryptanalysis or one of its related disciplines.

(U) Our outstanding group of judges considered the following criteria:

_____Was the talk an original discussion of a cryptanalytic subject?

_____Was the talk presented in a manner which made it easy to follow and understand? Was there a rapport between the

[redacted]

speaker and the audience? Did the speaker demonstrate enthusiasm for the subject matter?

_____Did the talk successfully serve as a vehicle for disseminating information about a relevant topic from the body of professional cryptanalytic knowledge?

(U) There were 15 entries:

- 3 from GCHQ
- 5 from NSA KRYPTOS talks
- 3 from CA305 talks
- rest were miscellaneous

(~~FOUO~~) On behalf of the KRYPTOS Society, I am very proud to announce the winners of our first Technical Talk competition. These pioneers have set standards which will be challenging for future competitors.

(~~FOUO~~) 3rd place [redacted] NSA $37.50
NSA $37.50
"Outsmarting A New Technology"

(U) This talk contributed significantly to the current body of knowledge on new technologies that are important to us at NSA. The talk was well-presented, providing a good introduction to the topic and extending beyond the basics. The use of state-of-the-art technology in their analysis was clearly described, demonstrating NSA's commitment to keeping up with the fast-paced technology changes in the world.

(~~FOUO~~) 2nd place [redacted] NSA $50
NSA $50
"The Challenge of (a new technical problem)"

(b)(3)-P.L. 86-36

(U) This talk was a very clear and interesting presentation of a topic that is/will be an important problem for NSA. It provided a good general overview of the worldwide scope of the problem in a well-organized and polished delivery. The talk contained a nice progression of simple examples which clearly demonstrated the ideas presented in the talk. The first and second parts of the talk complemented each other well, with the first providing ample motivation for the second.

(~~FOUO~~) 1st place [redacted] GCHQ $125
"New Mod-13 Arithmetic (for a specific problem)"

(U) The basis of the talk was a clever trick against an extremely important project. Additionally, the talk covered the use of a number of other well-known cryptanalytic techniques that are very important. It was delivered in such a way as to make the material easily understandable to those unfamiliar with the problem. The talk was highly organized, with excellent delivery and a wonderful economy of speech.

(~~FOUO~~) Congratulations again to all of our winners and a special thank you to our diligent judges. [redacted] who organized this competition.)

(U) The judges have commented that, although the decisions were not easy, they were very pleased that they independently arrived

[redacted] (b)(3)-P.L. 86-36

at the same choices, signifying that these talks are certainly outstanding and worthy of recognition.

3f. (U) Winners of 1998 KRYPTOS Literature Award

~~(TSC)~~ The Winners of the 1998 KRYPTOS Society Award have been announced as follows:

First place: [redacted]

Second place: [redacted]

Third place: [redacted]

Honorable mention: [redacted] ~~(TSC)~~ [redacted]

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(U) Congratulations to each of these excellent, cryptanalytic writers!

3g. (U) Call for Volunteers to Produce KRYPTOS Society Video

~~(TSC)~~ If you are interested in working on the KRYPTOS Society's new video project, please contact [redacted]. This is a unique and interesting opportunity to do a video from scratch--theme, planning, design, drafting text, interviews, working with the NSA TV Studio, etc. If you have always wanted to do something like this and would like to portray Cryptanalysis and the Cryptanalytic Community to a large audience, here's your chance. Videotaping interviews with recent retirees will definitely be a part of this project. Call [redacted] now!

(b)(3)-P.L. 86-36

3h. (U) Breakfast Affair for Newly Certified Cryptanalysts (BANCC)

This article is UNCLASSIFIED in its entirety.

Mark your calendars for the fifth annual Breakfast Affair for Newly Certified Cryptanalysts (BANCC).

Sponsored by KRYPTOS

Tuesday, January 26, 1999
8:00 to 10:00 a.m.

Keep on the lookout for more details of this popular event. Tickets will go on sale in January!

//

4. (U) COMMUNITY NEWS:

(b)(3)-P.L. 86-36

[redacted]

4a. ~~(FOUO)~~ Reprint of _CRYPTOLOGIC ALMANAC_ article:
Ernst Fetterlein (?1868-1944?)--For Tsar and King,
Cryptanalyst Extraordinaire,
by [redacted] (b)(3)-P.L. 86-36

(U) Revolutionary events in Russia in 1917 created great turmoil in the population and affected everyone, including the small band of cryptanalysts serving the Tsarist regime. Some of them, either voluntarily or involuntarily, remained in place and went on to serve the new Bolshevik regime: V.I. Krivosh-Nemanich and I.A. Zybine, both senior cryptanalysts from the Ministry of Internal Affairs' Department of Police; as well as G.F. Bulat, E.S. Gorshkov, Eh.Eh. Kartali, Eh. Morits and other (unnamed) individuals. (1) The remainder, who were the majority of cryptanalysts, either switched their allegiance to the anti-Bolshevik White forces or, apparently, dropped out of the cryptanalytic business altogether. However, only two individuals associated with the former Tsarist Russian cryptanalytic service have been identified to date as going to work directly for the cryptanalytic departments of foreign governments: P.A. Novopashennyj (2) for Germany and E.C. Fetterlein for Great Britain. Although both men were associated with Russian naval cryptanalysis during World War I, apparently only Fetterlein was a practicing cryptanalyst for most of his life. (3)

(U) Arguably one of Russia's and Britain's best cryptanalysts, Ernst Fetterlein remains an enigmatic figure even today to those who knew and worked with him in Russia and in the West. The information below on Fetterlein's life and career has been pieced together from the few available comments about him, mostly reminiscences from his former colleagues and acquaintances.

(U) RUSSIAN SERVICE

(U) Although little is known about the early life of Fetterlein, he probably was born in the mid- to late 1860s and entered into the cryptanalytic business as a young man in the early to mid-1890s. Two experienced Russian cryptanalytic contemporaries of Fetterlein, I.A. Zybine and V.I. Krivosh-Nemanich, had begun their cryptanalytic service with the Department of Police around the early to mid-1890s as well; Fetterlein's cryptanalytic service, apparently, was primarily with the Ministry of Foreign Affairs (MFA). Even when Fetterlein was later placed in charge of naval cryptanalysis during World War I, he remained an important figure in the MFA cryptologic structure by continuing to serve, as of 1915, on the MFA cryptologic committee of experts overseeing all cryptologic questions for the Tsarist Russian government. (4)

(U) Vladimir Korostovetz, a former private secretary to the Russian foreign minister, who was familiar with the work of MFA cryptanalysis, was highly impressed with Fetterlein's work in the MFA in the years before World War I:

> "We had men of real genius for this particular work, and of these the one who deserves to be mentioned in the first place is Fetterlein. Not only was he able to read all the telegrams written in the languages he knew, but he had brought his art to such perfection that he even read messages in languages of which he was quite ignorant, such as, for instance, Chinese and Japanese. These, after he had

(b)(3)-P.L. 86-36

[redacted]

deciphered the separate words, he would then hand over to the proper translators. A story is told how he was once sent to London with dispatches and was lunching at the [Russian] embassy. All through lunch he sat there dumb and almost sulky, when suddenly a change came over him and he began to chatter and laugh. One of the embassy officials asked what had happened, and then he confessed that he had been worrying over an undecipherable word he had come across in an English telegram, and that at this moment someone at the table had mentioned a shooting-box [hunting lodge] where the King was then staying, the name of which was the word that had been puzzling him." (5)

(U) Fetterlein really came to prominence at the outbreak of World War I with the Russian recovery of codebooks and other material from the German cruiser _Magdeburg_, which had run aground near Odensholm (now Osmussar) Island in the Baltic on 26 August 1914. Successful initial efforts at cryptanalysis of German naval communications led the Tsarist Naval General Staff (NGS) to launch a more systematic effort and to concentrate the effort at the Shpitgamn (now Cape Poosapea) radio intercept station in Estonia. The NGS selected Fetterlein from the MFA to lead the effort, assisted by a number of naval officer-cryptanalysts. Due to his German-sounding last name, Fetterlein was assigned the name of "Popov" to use until the war ended.

(U) The intercept site itself was very isolated, located in the middle of a cleared-away pine forest, with an operations building and another one for living quarters of the assigned personnel. Although life at the site was spartan and no contact was allowed with the outside world, numerous "courtesies" were extended to Fetterlein for his cryptanalytic services by the NGS and Baltic Fleet command. Fetterlein was not only allowed to bring his wife to live at the site (no naval officers stationed there were permitted to do so), but also a house was specially built at the site for the couple. (6)

(U) The naval officers who worked with Fetterlein, according to a former high-ranking Tsarist navy official, were also most impressed by his cryptanalytic abilities:

"...In the words of those officers who worked together with him, the capabilities of this man for breaking any cipher were frankly amazing. There wasn't one case where he, after spending several hours of work in total solitude, couldn't find the key for breaking the unknown cipher as if it weren't new and complex." (7)

(U) The high regard for Fetterlein and his cryptanalytic abilities, by government and naval officials during World War I, was continually enhanced with each successful decryption of German naval communications. One example, according to a former government official, involved plans for a major attack by the German navy in the Baltic:

"...During the war an intercepted wireless message was handed to him to decipher. It was from the German Fleet, and he discovered in it a detailed order for an advance on all lines towards the Gulfs of Finland and Riga, in order to carry out an attack against the Russian Fleet. Thanks

(b)(3)-P.L. 86-36

Doc ID: 6823826

to Fetterlein's work our Fleet was therefore enabled not only to take defensive measures, but to send minelayers; one of these even advanced far enough into the Bay of Danzig to write a message on a cliff there. The attack of the German Fleet did not succeed, and on their retreat several ships were sunk." (8)

(U) BRITISH SERVICE

(U) Following the outbreak of revolution in Russia, with all its accompanying danger and uncertainty, Fetterlein apparently decided to leave the country to go abroad in 1918. One of his former colleagues in World War II at Britain's Government Code & Cipher School (GC&CS) (predecessor of the Government Communications Headquarters/GCHQ), P.W. Filby, later recalled what Fetterlein had to say about this period:

"...as the top cryptographer in Russia he had the rank of Admiral, and his stories of the day the Revolution occurred, when workmen stripped him of his many decorations and bullets narrowly missed him, were exciting. He escaped Russia in a Swedish ship which was searched by the Russians, who failed to find Fetterlein and his wife. It is said that the French and British organizations were anxious to get him, and Fetterlein simply sat there and said, 'Well, gentlemen, which will pay me the most?'." (9)

(TSC) Fetterlein apparently decided that Britain offered the best opportunity, if it wasn't his first choice all along, and in 1918 he joined GC&CS. He was subsequently placed in charge of the cryptanalytic effort against the ciphers of the new Soviet regime in Russia. A close friend of William F. Friedman and a contemporary of Fetterlein at GC&CS, the legendary cryptanalyst Brigadier John H. Tiltman, later described his association with, and impression of, the man during the early 1920s and late 1930s:

"[Upon being attached to GC&CS in August 1920]...I worked as one of a group of from 5 to 7 persons on Russian diplomatic ciphers under the direction of Ernst Fetterlein. Fetterlein had been Chief Cryptanalyst of the Russian Czarist Government and held the ranks of both admiral and general (10); he had practiced cryptanalysis since 1898 or earlier. At the Revolution he walked out of Russia across the Finnish frontier and was specially naturalized on arrival in England....it used to be said in GC&CS in 1920-1921 that I was the only person Fetterlein had ever been known to help....[by 1939]...Ernst Fetterlein was still in my opinion far the best general-purpose cryptanalyst." (11)

(U) Although he had left Russia in 1918, Fetterlein was still on the minds of the new Russian leaders. By the end of 1920, if not before, the Bolshevik leadership, including Lenin himself, were aware of Fetterlein's cryptanalytic activities on behalf of the British in supporting the anti-Bolshevik White Russian forces during the Russian Civil War. (12) The head of GC&CS, A.G. Denniston, later noted that at that time the only real operational intelligence obtained by GC&CS came from the work against Soviet Russian traffic, and Ernst Fetterlein was a major part of the effort:

"...The presence of Fetterlein as a senior member of the

(b)(3)-P.L. 86-36

staff and two very competent girls, refugees from Russia, with a perfect knowledge of the language, who subsequently became permanent members of the staff, enabled us to succeed in this work. (13)

(U) Fetterlein continued to be active for the remainder of the 1920s and 1930s until his retirement from GC&CS in 1938. However, his retirement was brief. When war broke out again in 1939, he returned to work.

(S) In May 1943, William F. Friedman met with Fetterlein (or "Vaterlein" in German, as Friedman mentions him) during World War II, while on a visit to Great Britain, and had the following to say about him afterwards in his diary:

"...Met Mr. Vaterlein, dean of crypt, who is over 75 and has been in work for 50 years. Told me R's [Russians] adopted 1-time syst in 1916-17. RFO [Russian Foreign Office] had staff of 5 beginning back in '96. Austrians most clever and told R's pointers. Systems all very simple 1-part cdes which remained in effect for long time. Norway, for exple, used same one from '93 to 1940. V is still quite active mentally and gets quite kick out of reconstruct 2-pts. He doesn't care for 'machines'." (14)

(U) Friedman also understood Fetterlein's value as a cryptanalyst under the former Tsarist Russian government, when he later commented on a gift given to Fetterlein by his former employers:

"...I vividly recall that he wore with great pride on the index finger of his right hand a ring in which was mounted a large ruby. When I showed interest in this unusual gem, he told me that the ring had been presented to him as a token of recognition and thanks for his cryptanalytic successes while in the service of Czar Nicholas, the lathe line." (15)

(U) Even though Fetterlein was now in his seventies, his new, younger World War II GC&CS colleagues still considered his cryptanalytic abilities to be quite good, and he continued to use his skills, literally, until the last days of his life, according to P.W. Filby:

"...He was a brilliant cryptographer, but like the older civil servants he had not been involved in machines and more up-to-date systems. Thus on book ciphers and anything where insight was vital he was quite the best. He was a fine linguist and he could usually get an answer no matter the language....When Fetty became ill in his seventies, I took problems to him at Kew, and with a good safe and a very understanding wife he did wonders for us in the last months of his life. Present-day officers would be horrified at this, but if I could have placed a plaque on my door it would have had the phrase, 'The end justifies the means'. Finally Ernst Fetterlein died [probably around 1944]. I called to express the condolences of the Foreign Office and to collect papers...." (16)

(U) POSTSCRIPT

(b)(3)-P.L. 86-36

(U) COMMENT: The life of Ernst Fetterlein, in almost equal service to both Russia and Great Britain during the momentous events of the 20th century, might seem to some fiction writers as almost unbelievable. As a cryptanalyst and witness to events affecting both countries, he truly occupies a unique historical place and will probably continue to remain the enigmatic and interesting figure in death that he was in life.

(U) FOOTNOTES AND SOURCES

(1) (U) T.A. Soboleva, _Tajnopis' v Istorii Rossii_ (Cryptology in the History of Russia), Moscow, 1994, 325-327.

(2) (U) Novopashennyj's prior career included a stint as a professor of astronomy, chief of Baltic Fleet communications (and intelligence) service in 1917, chief of intelligence/ counterintelligence for the White Russian naval forces in northwest Russia in 1919 and, from 1921 through World War II, head of Russian cryptanalysis in the German Reich War Ministry Cipher Center. See [redacted] "Communications Intelligence & Tsarist Russia," (NSA) _CRYPTOLOG_, January 1984, 7,12, and W.F. Flicke, _War Secrets in the Ether: Part II_, Laguna Hills, CA: Aegean Park Press, 1977, 292-293.

(3) (U) [redacted] "Russian Naval COMINT Activity, WWI and WWII," _CRYPTOLOGIC ALMANAC_, 18 June 1998.

(4) (U) [redacted] "Part I: Russian MFA Cryptologic Organization, Late 19th - Early 20th Century," _CRYPTOLOGIC ALMANAC_, 19 October 1998.

(b)(3)-P.L. 86-36

(5) (U) V.K. Korostovetz, _Seed and Harvest_, London, 1931, 220-221.

(6) (U) [redacted], "The Magdeburg Incident: Russian Intercept and Cryptanalytic Efforts in World War I," (NSA) _CRYPTOLOG_, April 1984, 18-22.

(7) (U) Rear Admiral S.N. Timirev, _VOSPOMINANIYA MORSKOGO OFITsERA_ (Recollections of a Naval Officer), New York, 1961, 46-47.

(8) (U) Korostovetz, _Seed and Harvest_, 221.

(9) (U) P.W. Filby, "Bletchley Park and Berkeley Street," _INTELLIGENCE AND NATIONAL SECURITY_, London, April 1988, 280.

(10) (U) Fetterlein may have held an even higher position. According to the Tsarist "table of ranks," the naval rank of "General-Admiral" was the equivalent of an army "Field Marshal"--a good indication of the value placed on the cryptanalytic services rendered by him. See "Tsarist Table of Ranks," _VOENNO-ISTORIChESKIJ ZHURNAL_ (Journal of Military History), Moscow, June 1978, 119-120.

(11) (TSC) J.H. Tiltman, "Experiences 1920-1939," _NSA TECHNICAL JOURNAL_, Summer 1972, 1,3,5, and 9.

(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

(12) (U) [redacted] "Part II: Soviet Ciphers and Knowledge of British Cryptanalysis during the Russian Civil War (1918-1921)," _CRYPTOLOGIC ALMANAC_, 21 October 1998.

(13) (U) A.G. Denniston, "The Government Code and Cypher School Between the Wars," _INTELLIGENCE AND NATIONAL SECURITY_, London, January 1986, 55.

(14) ~~(S)~~ "Diary of William F. Friedman, 23 April - 13 June 1943," (NSA) _CRYPTOLOGIC QUARTERLY_, Summer-Fall 1982, 25.

(15) (U) W.F. Friedman, "Six Lectures on Cryptography," April 1963, 118, National Archives, Washington, RG 457 SPH-004, cited in C. Andrew and K. Neilson, "Tsarist Codebreakers and British Codes, " _CODEBREAKING AND SIGNALS INTELLIGENCE_, London, 1986, 10-11.

(16) (U) Filby, "Bletchley Park and Berkeley Street," 284.

4b. (U) Women in Mathematics Symposium (WiMS) Calls for Volunteers

4b1. (U) EVENT: Math Talk at the University of Puerto Rico; date unspecified

~~(FOUO)~~ WIMS POC: [redacted]

(U) The University of Puerto Rico would like to have a female mathematician with a Ph.D. visit them sometime during this school year to give a talk. This is all the information we have at this time. Once someone volunteers, she can work with WiMS and the university to determine the details.

4b2. (U) EVENT: Math Talks for students and faculty at the University of Akron; April, 1999

(b)(3)-P.L. 86-36

~~(FOUO)~~ WIMS POC: [redacted]

(U) The math department at the University of Akron (Akron, Ohio) would like a female NSA mathematician to visit them for 1--2 days during the second or third week of April 1999. They would like the volunteer to participate in a number of activities including (1) presenting an undergraduate mathematics colloquium, (2) meeting with math students to discuss career opportunities at NSA, and (3) attending a luncheon meeting with women math students and faculty. The department typically operates these sessions on a Wed/Thur or Thur/Friday, but the scheduling is flexible.

~~(FOUO)~~ If you're interested, please contact [redacted] 963-4897), [redacted] or [redacted] for more information.

(b)(3)-P.L. 86-36

[redacted]

4c. (~~FOUO~~) Greetings from Cheltenham Chapter
by [redacted]

(~~FOUO~~) If you can get to the [redacted] you may be able to access the web pages of the Cheltenham chapter of the KRYPTOS Society. The URL is: [redacted]
(U) There you will find copies of our recent newsletters, along with other KRYPTOS information, such as talks and social events, awards and prizes, distinguished members' biographies, puzzles and problems, and the entries of the 1998 Cryptanalytic Limerick Contest.

(~~FOUO~~) * This worked for me with Netscape on the NSA web: under network preferences, under proxies, click automatic proxy configuration and for the url enter: [redacted]
and hit OK.

(b)(3)-P.L. 86-36

4d. (U) The Operations Research Career Panel Presents the January 1999 Technical Social: "Confidence Scoring in Speech Recognition: Logistic Regression at NSA" by [redacted]

(U) This talk will be presented on 7 January 1999, at 1:00-2:30 p.m. in the D5 Conference Room, OPS2B, Room 2B4118-2.

(U) ABSTRACT:

(U) Large Vocabulary Continuous Speech Recognition (LVCSR) systems are used to convert incoming speech signals into readable text. Unfortunately, the output of LVCSR systems can be highly errorful, with word error rates of approximately 70% in some applications. This level of performance will have an adverse effect on the assessment of the intelligence of intercepted speech. Confidence scoring methods, which provide an estimate of the probability that a recognized word is correct, can be used as a processing filter to separate likely correct word output from that which is likely erroneous. Intelligence value assessment can then be conducted on the filtered output. In this presentation, the author will demonstrate the use of logistic regression to provide confidence scores for LVCSR output. Confidence scoring models that have been developed using an unclassified speech corpus will be evaluated on intercepted speech target. Other statistical methods for confidence scoring, and alternative evaluation metrics of model performance will also be discussed.

(U) About the Speaker:

(~~FOUO~~) [redacted] has over 13 years of experience as a statistical consultant, and worked on a variety of projects related to operations research. [redacted] has published over ten articles in peer-reviewed journals as lead or co-author, along with over thirty reviewed reports to clients. [redacted] has presented research at meetings of The Biometric Society/American Statistical Association, and Envirometrics 87, along with meetings of government managers from the Federal Government (EPA), state governments of Maryland, Virginia, New Jersey), and industry (Consolidated Edison of NY, NYPA).

(b)(3)-P.L. 86-36

[redacted]

(U) Light refreshments will be served!!! (b) (6)

5. (U) TECHNICAL HEALTH

5a. (~~FOUO~~) Chromosome Classification by [redacted] IDA/CCS, [redacted] University of Maryland, College Park, and [redacted] Oak Ridge National Laboratory

(U) Basic assembly instructions for living beings are carried in the organism's cell nuclei as chromosomes. Humans, for example, normally carry 46 chromosomes: 22 pairs of autosomes (numbered 1 through 22), and two sex chromosomes (XX for females and XY for males).

(U) Chromosomes consist of a sequence of genes plus specialized elements such as a centromere, important in cell division. Each gene is a sequence of nucleotide bases that carries the code for constructing a protein. These proteins form the building blocks for cells and enzymes. Chromosomes can be seen under a microscope stained with dyes to reveal a distinctive pattern of light and dark bands.

(U) Determining the identity (e.g, 1-22, X, or Y) of a chromosome is called karyotyping. Karyotyping is important in diagnosing cancer, finding damage due to environmental factors, and detecting genetic abnormalities. For example, Downs syndrome is diagnosed by determining that each nucleus contains a third copy of chromosome 21. Karyotyping is tedious and repetitive if the process is manual. Even partially automatic methods are of great help to technicians.

(U) In our work we have investigated several classification methods. Here we will highlight two methods. The method is principal component analysis. Both methods will require several thousand samples of digitized images of chromosomes. For the purpose of experimenting the data will be divided into a training and scoring subset. For each entry in the data we have a sequence of gray scale values from the image and a 30 long feature vector, consisting of the number of bands detected, length of chromosome, perimeter of the convex hull, and weighted gray scale densities. Both data items are readily computed automatically from the image and are standard in karyotyping.

(U) The feature vectors will be modeled as sampled from 30 dimensional multivariant normal distribution. For simplicity we assume that while each chromosome has its own mean vector we assume that they share a common covariance matrix. Furthermore, we assume that the covariance matrix is rank 24. Thus, we have a principal component linear discriminant model. This model can correctly classify a chromosome about 95% of the time. Under the assumption that each chromosome occurs at most twice and either XY (male) or XX (female) are the only sex chromosomes present, then a linear assignment (a special case of linear programming) can improve the results to about 97%.

(U) We use a hidden Markov model (HMM) to model the variable length of the sequence and to account for shrinking due to bent or cut chromosomes. The Markov chain is simply a forward only model which allows for one insertion or deletion per time step. The rows of the

output matrix (B-matrix) are assumed to be normally distributed. Given the training data 24 HMM's can be built. This model is particularly good at identifying shortened chromosomes. Preliminary testing indicates the HMM model degrades by a couple of percent in its classification error rate, when the chromosomes are missing their first 10% of their gray scale values.

5b. (~~FOUO~~) Summary of Recent [redacted] Developments (b)(3)-P.L. 86-36
by [redacted] Z233

(~~FSC~~) [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

5c. (U) Technical Reference Guides

~~(C CCO)~~ Z6 is continuing to add new titles to its Technical Reference Guides (known as trifolds). The latest addition to this growing list is entitled [redacted]

(b) (1)
(b) (3)-P.L. 86-36

~~(FOUO)~~ [redacted] The trifolds were originally intended as summarizing handouts to accompany briefings by experts to Seniors, budget analysts, congressional staffers, and others involved in the SIGINT business, but not themselves experts in the area covered. This series is now available to all cleared personnel.

(b) (3)-P.L. 86-36

~~(FOUO)~~ The trifolds are available for viewing or downloading from the NSA WEB or accessible from the Z644 HOMEPAGE. All the trifolds may be viewed on-line at: [redacted]

~~(FOUO)~~ Requests for printed copies may be submitted via an ordering form at: [redacted]

//

6. ~~(FOUO)~~ PUZZLES
by [redacted] Z841

(U) Solution to September-October Puzzle - Say What?

(b) (3)-P.L. 86-36
(b) (6)

[redacted]

(U) Following are a number of series of words that look like gibberish, but if pronounced correctly, sound like a meaningful phrase. An example of this is the code signature used by one of the U.S. Presidents. He wrote: Ale In Can, which when pronounced in a slightly twisted way, reveals A. Lincoln. Have a go at these. Because they're a little odd, a category is provided to help guide your search.

(b) (3)-P.L. 86-36

Category Words to Decode

[redacted]

Physics Phenomena	Arm, moniker, moe, shun
Book Title	Bate, Riyadh, gay, aims
Physics Formula	Effie, quill, Sam, May
Physics Concept	Eyes, umber, guns, ardent, deep, rinse, sable
Disney Saying	Hack, unum, mitt, ta-da
Shakesperean Play Quote	Hoe, why, yams, lain
Book Title, in French	Lipid, deep, rants
Shakesperean Character	Omelette, print, soft, tan, mock
World Leader	Poe, budge, on, ball, thus, sack, end
Literature Title	Thud, eh, though, fee, Vanilli, itch
Musical Title	Vent, a, muff, tee, up, bra
Cartoon Characters	Yak, cow, walk, owe, went, tot

Answers in order:

Harmonic Motion
Patriot Games
F=MA
Heisenberg Uncertainty Principle
Hakuna Matada (from "The Lion King")
O, I am slain! (Caesar)
Le Petit Prince
Hamlet, Prince of Denmark
Pope John Paul II
The Death of Ivan Ilyich (Dostoevsky)
Phantom of the Opera
Yakko, Wakko, and Dot (animaniacs)

(FOUO) Solutions were provided by: [redacted]

6b. (U) November-December Puzzle - Annual "KRYPTOS KRISTMAS KWIZ" (b)(3)-P.L. 86-36

(U) KRYPTOS KRISTMAS KWIZ 1998

(FOUO) [redacted] have once again put their warped minds together to produce the 1998 "KRYPTOS Kristmas Kwiz." As usual, some questions are more difficult than others, so each has an associated Warp Factor. For factors greater than 1, points may be awarded for a nearly-correct answer or even a gallant effort, so enter something on the answer sheet even if you're not sure. And if your answer is better than ours, you may receive bonus points. The Kwiz is designed to be quite hard (in places), and some questions may be impossible thanks for [redacted] Overwarp or [redacted] Wisprint (though we have tried our best to avoid this!), so do send in your answer sheet even if it's not complete.

(U) Webster's Dictionary will be taken as the authority for what constitutes a "word." If your answer includes an obscure word which is not in Webster's, but in some other common dictionary, tell us which. Unless otherwise stated, "words" do not include proper nouns or entries which include punctuation, including hyphen or apostrophe.

(FOUO) NSAers should e-mail responses to [redacted]. Those at GCHQ should follow their own instructions. The names of the winner(s) and all contestants who received a score of greater than zero will be (b)(3)-P.L. 86-36

[redacted]

published in a forthcoming _Tales of the KRYPT_. The deadline for responding is COB Friday, January 29.

So, good luck, and have fun!

(U) 1. Where does WEST fit in the following list (read across):

MEAL	HOPE	COPY	GRANT	NAP	BOW	TOGETHER	
SEASON	BEECH	SLIP	TRIPPER	WOOD	DAY	ROAD	
GLOVE	BACK	STANDARD	PECK	GOODBYE	PLAY	CURTAIN	
CANDY	MADONNA	PENCIL	BALL	LIGHT	REPLY	MAN	
MASK	WRITER	IRON	PUNCH	RACCOON	MILL	EARTH	
DIP	TEMPLE	CROSS	LINING	BEST	TONGUE	LILY	
SOLDIER	ICEBERG	CRUISE	CENTURY	MARK	WHISTLE	SUBMARINE	(5)

(U) 2. And where does EARN fit in the following list:

PATRONAGE	NEARLY	WINDY	BRIBE	MINIATURE	FRAGMENTS	HAZARD
ACT	DIVINITY	OBSCENE	BITES	8	COLLAPSES	40
4	SPIRIT	RENOWN	RELIGIOUS	EQUINE	STATUES	CANOE
EVEN	SORCERY	GRASS	IRISHMAN	GRAIN	FRESH	ROW
GLIMPSE	FOLDS	MINISTER	CHARLATAN	NAUSEATED	RAN	ROSIER
ASSIGN	STRAIGHT	STORIES	MERMAID	POSITION	FUMES	AVOID
CONFESS	ASTERISK	PROSPERITY	OPINION	FOOTPRINT	2	EXHAUST

(5)

(U) 3.(a) a set of words has a constant "tail" preceded by a prefix. The prefixes for the fifth, sixth .... tenth words are appropriate, but those for the first .... fourth words relate to "wine", "sky" etc. What is the third word of this series? (1)

(b) in another set, the first two "words" are missing, because they cannot exist. The third and fourth words exist, but are almost invariably replaced by words with a different tail. The fifth, sixth ... tenth are normal. What is the third word of this series? (1)

(c) a third set contains words with the prefix representing 7-, 8-, 9- and 10-, but apparently with the wrong values, and no other member of the set has a numerical prefix. What is the third word of this series? (1)

(d) and a fourth set has appropriate prefixes for 2, 3, 4, etc. but the tail for 1, 2, 3 is different from that for 4, 5, 6 etc. What are the two tails? (1)

(U) 4. An Agram is an N-letter word, with no repeated letters, which can give rise to N words using the N letters plus each letter repeated, in turn. For example, SEL leads to LESS, EELS and SELL.

(a) Find a 4-long Agram (1)
(b) Find a 5-long Agram (1)
(c) Find a 6-long Agram (2)

(U) 5. A reference book contains a list of 11 things, in order; each thing is followed by two parameters. Unfortunately, as we copied them, each character of each parameter was replaced by a different character. The first column became LIE, PSI, IAR, ASH, AER, EIL, ERP, HI, PA, OH, AT. The second became EELS, LIE, PSI.....OH.

(a) what was EELS before the transformation? (1)
(b) what are these things? (1)

(b)(3)-P.L. 86-36

Doc ID: 6823826

(U) 6. Each of the following lists contains a number of words which have a strong common property, and one which has a similar, but distinctively different property. Which are the odd men out?

(a) AVENUE BINDER COURAGE FORTUNE LEMUR MERCHANT NONPLUS TRESPASSER (1)
(b) CLAPPER CLUMPS DELUGING DEPART DOLMENS HANDSOME SMILED STEADY TELEGRAPHIC (1)
(c) DEMERGE EMANATE GRATIN HUNTERS MALAR OVERS RAMBLE SPOTTER TRIO WANE (1)
(d) APPEARS COMATOSE ECLIPSE EFFETE JEOPARDISE NECROMANCY PURISTS RICHEST URCHIN VENOSE (1)
(e) ALLIANCE BARGAINED CROUPIER ENGAGES PRICKLE PROTOPLASM SHANTIES SITUATION STINGING THANKLESS (2)

(U) 7. What is the next number in the following sequences:

(a) 1, 2, 4, 7, 12, 20, 33, 54, 88 (1)
(b) 2, 2, 2, 3, 2, 2, 4, 2, 3 (1)
(c) 4, 2, 5, 2, 6, 10, 3, 7, 6, 4 (1)
(d) 1, 2, 3, 2, 1, 2, 3, 4, 2, 1, 2, 3, 4, 3, 2 (1)
(e) 155, 186, 203, 290, 299, 323, 348, 506, 578 (2)

(U) 8. We gather that everyone hated the word series last time, so here are some more! What word can follow:

(a) EMPTY CELLS THEFT STREW (1)
(b) JACKAL MILKED MEANLY YEOMAN SPOONS (1)
(c) STOP LUMBERED TORN DENOTED CONTORTS TUBERS NUTHATCH BARRISTERS DITHERS (1)
(d) ME ROW MAIL SWOON JACKAL PRONOUN AMICABLE PROTOZOON (1)
(e) ENOUGH WORTHY REHEAT FURROW VERIFY EXISTS (1)
(f) WISTFUL NOTABLE BELIEVE EXTRUDE FURLONG PANACHE (1)
(g) OPENED SECURE SUMMIT BEFALL ISOBAR LATTER INSECT OVERDO SECRET (1)
(h) TINE PLUM SERA HEAR FORT BRIE CLAN CLOT (1)
(i) PIECE LADDER HASTE EMOTION BONY LITTER RASPING ARROW RISES (1)
(j) LOT CHE CAT SHE LAR SAY ESS LEE ASP RED CIT REE (1)
(k) SQUELCH PARTING TUMBLED MARXIST EMPTILY SPLAYED DETAILS INSTEAD (1)
(l) RIGHTS ZONAL APPEAR PETER YOUTH MINA TWIST PEAL DEEP HIT JUGS DAY OUT (1)
(m) INEPTITUDE WIZENED REDISTRIBUTE VERIFY FUNFAIR CHESSBOARD BIENSEANCE CHATTERBOX (2)
(n) CHLORINE TUXEDO EXAMPLE EFFECTS CENTRE VERMOUTH POSSESSIVE NOTE AUSTRALIA ADDITION GOD BRITAIN (2)
(o) IF TEN KNOT VIXEN ARCHER PARAPET INCLINED REDELIVER INSPIRATOR (2)
(p) WANDER BREATH LYRIC NAIAD GRADE FARED REGARD THREES (2)
(q) SURGERY AVOIDING FALLBACK LINGERED PATRONAGE ANCESTRAL TROUBLE UNDERNEATH (2)

(U) 9. The digraphs representing the US states are AK AL AR AZ CA CO CT DE FL GA HI IA ID IL IN KS KY LA MA MD ME MI MN MO MS MT NC ND NE NH NJ NM NV NY OH OK OR PA RI SC SD TN TX UT VA VT WA WI WV WY. What is the longest word which can be formed, without reusing digraphs within a word, by:

(a) stringing together the above digraphs - e.g. DE-CO-CT (1)
(b) chaining - e.g. FLAKY: FL/LA/AK/KY (1)

(b)(3)-P.L. 86-36

(U) 10. Replace each question mark in the following series by a digit

7 4 ? ? 2 3 9 6 2 1 5 (1)

(U) 11. My first is in first but not in seventh
My second is in third but not in ninth
My third is in fifth but not in second
My fourth is in sixth but not in eighth
My whole is what's missing, which spoils it.
What am I? (1)

(U) 12. Which number is the odd one out:

(a) 111, 215, 334, 431, 666, 951 (1)
(b) 251, 334, 512, 621, 625, 972 (1)
(c) 246, 258, 741, 753, 951, 987 (1)
(d) 258, 294, 438, 555, 618, 951 (2)

(U) 13. Each entry in the following lists leads to another entry, in a manner which you are to determine, and this second entry leads to a third, in a different manner. These third entries are in alphabetical order. What are they?

(a) ALLEY, DESERT, POLAR, CRY, HOT, LOAN, MARCH, SEA, LEMON, SCREECH, SHIRE, ROLLER (1)
(b) THE HAGUE, VALETTA, ANKARA, MADRID, HAVANA, PARIS, LISBON, COPENHAGEN, BERNE, MOSCOW, BERLIN, NEW DELHI, BEIJING (1)
(c) CENT, HEAVEN, FOOL, HAMLET, ATTITUDE, MECHANICAL, OUTRAGEOUS, DIOCESE, VOLITION, BRASSICA, RIPE (1)
(d) RICH, HAIRY, WARM, CROOKED, ALIVE, DARK, UNWELL, SANE, LOW, UGLY, FAT (1)

(e) COCK, BED, FAG, TELL, WRAITH, FROM, TOP, METRE, NAME, RUNG, BOOK (2)

(U) 14. Seven words have been enciphered using a simple substitution. Decrypt them, and then put them in the appropriate order:
FRAFR CNEGL THRFF URNIRA RFGNGR YNQL PBYHZA (1)

(U) 15. Using just the NATO phonetics (ALFA BRAVO CHARLIE DELTA ECHO FOXTROT GOLF HOTEL INDIA JULIET KILO LIMA MIKE NOVEMBER OSCAR PAPA QUEBEC ROMEO SIERRA TANGO UNIFORM VICTOR WHISKEY XRAY YANKEE ZULU) what is the longest list of different words you can find such that there are exactly three repeated letters between each adjacent pair of words. Note that there are three repeats between WHISKEY and YANKEE, not 4, and three between NOVEMBER and YANKEE (N and 2 E's). (1)

(U) 16. (This question celebrates the continuance of Round Britain Quiz on BBC Radio 4): The format is one, long, cryptic question which has six parts to it, indicated by the letters a-f. To gain full marks you should identify all six parts. This will be sufficient to answer the question!

Identify the major sixth of the scale of C (a); an elevated railroad (b); the nutritious seed of Pisum Sativum (c); and Planck's constant (d). Together (e) they run down to something that is perpetually dark (f). How is this? (3)

(U) 17.

(b)(3)-P.L. 86-36

Doc ID: 6823826

(a) Explain the geographical sequence which begins:

96 126 168 784 1404 1638 2240 2268 2730 2754 2912 2940 3024
3120 3420 3510 4050 4536 4860 5400 6084 6120 8232 ..... (2)

(b) Why is 3024 unique in the part of the sequence shown above? (1)

(c) Find another number, a little later in the series, with the same property as 3024. (1)

(U) 18. Which 6-letter word connects the following:

TPSSPX, LQA, JLUO, FSC, XNQAJW, MURJ, ZLJYLA ULCLY AV IL AVSK (1)

(U) 19. The spaces have been lost between the letters (and words) of the following Morse Code phrase. What does it say?

_ . . _ _ _ _ . . . . _ _ . _ . . _ . . _ . . . . . .

A . _	B _ . . .	C _ . _ .	D _ . .	E .	F . . _ .
G _ _ .	H	I . .	J . _ _ _	K _ . _	L . _ . .
M _ _	N _ .	O _ _ _	P . _ _ .	Q _ _ . _	R . _ .
S . . .	T _	U . . _	V . . . _	W . _ _	X _ . . _
Y _ . _ _	Z _ _ . .	(1)			

(U) 20. DOSH, HOWL, MANO, OTIC, POET and WAXY have a common property (other than being 4-long). There's another 4-long word with the same property, which can be preceded by a 3-long word with the same property. What are they? (1)

(U) 21. What is the next matrix in this series:

(1 1) (2 2) (5 4) (3 7) (5 5)
(1 1), (1 3), (3 2), (8 4), (9 16)
(2)

(U) 22. Each letter of the alphabet is associated with a non-zero digit, and the score for the following words is the sum of the digits associated with each letter:

RATE 12 SOUP 12 ADORE 13 DARTS 13 HEARTY 15 READS 15
THING 19 POLISH 23 KNIGHTS 24 SPOILS 24 PURPOSE 25

a. What is the score for KRYPTOS? (1)
b. If POPPY is 20, what is the score for RETREATING? (1)

(U) 23. What is the next pair of numbers in the series:

(18,19), (28,29), (38,39), (79,80), (81,82), (83,84), (85,86) (1)

(U) 24. What is the next in these series:

(a) E, R, T, ED, EP, CE, CO, RT, YP, PP, TT, IO (1)
(b) A, j, Cb, UJ, ACO, CAU, FJF, OAC (2)

(the lower case letters are deliberate)

(b)(3)-P.L. 86-36

(U) 25. I have in front of me 100 letters in a 10x10 table. The

letter count is:

A:	17	B:	2	C:	2	D:	2	E:	7	F:	0	G:	3
H:	5	I:	10	J:	0	K:	1	L:	5	M:	7	N:	4
O:	7	P:	8	Q:	0	R:	2	S:	4	T:	8	U:	4
V:	0	W:	0	X:	1	Y:	0	Z:	1				

Some of the words/prefixes in the table are shown below:

.	.	.	H	.	.	.	.	.	.
.	.	M	A	D	E	.	T	.	.
.	.	.	L	.	.	.	E	.	.
.	T	.	T	.	.	.	A	.	.
.	A	.	A	P	P	A	L	.	.
.	D	.	.	.	.	.	.	.	.
.	.	.	.	.	N	.	.	.	.
.	.	.	.	.	A	.	.	.	.
.	.	.	.	.	N	.	.	.	.
H	I	P	S	.	O	.	.	.	.

Deduce the positions of the remaining letters: what 4-letter prefix appears at the right end of the bottom row? (2)

(U) 26. What is the last word in the following:

SOMETHING PECULIAR HAPPENED WHEN I SAT DOWN
RI YSW RHW RTOWQEURWE. RHW FAYLR GIR QIESW
YNRUK RGW RWXR CIYKD NIR BW EWCIFNUAWS. UR
AWWNWS RI VW XINOKWRW FIVVKWSTFIIJ.

(U) 27. A WordPair is a pair of words which have no repeated letter either within them or between them (e.g. FORD and GULP). Find the WordPair which maximizes the product of their lengths. (3)
(U) 28. Each of two related words is clued by two one-word definitions, but the order of these four words is random. There are seven such pairs of words. The relationship between each pair of words will help identify one letter from each word: when arranged in the right order, side by side, the letters will spell out a well-known name, column by column. The clues are:

DOCTOR PASSENGER COOK FOOD
CRAM CREDIT BEAT FOLD
DIM DRAW STRETCH BLUNT
ASTUTE COMMAND WISH CRAFTY
DULL IGNORANT OBSCURE MILD
PURIFY SUBTLE IGNITE ENTHUSIASM
HAZARD PASSION INSECURITY ANGER

What is the name? (2)

(U) 29. Converting the letters into numbers (A=0, B=1 ... Z=25), and treating the alphabet as cyclic, I can subtract one n-long sequence >from another to form another sequence of the same length. For example, WILLIAM CLINTON could be UXDYPMZ. Who are:

(a) AAACAAR (1)
(b) PTEYTPZ (1)
(c) TTRNYKAC (1)

(An actor and a couple of leaders - though not necessarily, of

(b)(3)-P.L. 86-36

course, in that order.)

(U) 30. Decipher the following. What is the longest word in the message?

AMPER TROYC AHERI OSATM HANSA ENIDA SHRAP EPOYN SELWY DEGAR (1)

(~~TOUO~~) Please send all solutions, as well as new puzzle ideas, to [redacted]

7.(U) EDITORIAL CORNER

REMINDER: (U) Submissions for the next issue are due by 28 December.

PLEASE NOTE: (U) All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION-MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the editorial board.

(~~TOUO~~) EDITORIAL BOARD

[redacted]

Jack Ingram, Cryptologic History Museum, [redacted]

[redacted]

(b)(3)-P.L. 86-36

~~TOP SECRET UMBRA~~

Derived from: Multiple Sources
24 February, 1998
Declassify on X1, X3, X5, X6, X7, X8

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

(b)(3)-P.L. 86-36

[redacted]

~~SECRET//COMINT~~

~~(S)~~ POC: [redacted] *info*

(U) *Last Modified: 10/30/2002 11:42:24*

(U) PE EXTERNAL PAGE

~~SECRET//COMINT//XI~~

[redacted] (b)(3)-P.L. 86-36

****
* TALES OF THE KRYPT *
****

January - February 1999

//
****

++
//

(U) TABLE OF CONTENTS:

1. (U//~~FOUO~~) PERSPECTIVE: "Changes," by [redacted]

2. (U) CALENDAR OF EVENTS

3. (U) CRYPTANALYSIS CAREER PANEL NEWS: Breakfast Affair for Newly Certified Cryptanalysts (BANCC)

   3a. (U//~~FOUO~~) Text of [redacted] BANCC Speech

   3b. (U) BANCC Newly Certified Cryptanalysts

4. (U) KRYPTOS SOCIETY NEWS: 1999 KRYPTOS Society Officers

5. (U) TECHNICAL HEALTH

   5a. (~~C//SI~~) Understanding 56k Modem Technologies by [redacted] (b)(3)-P.L. 86-36

   5b. (U) DO Technical Health Advisory Board Special Achievement Awards

6. (U//~~FOUO~~) LETTER TO THE EDITOR, from [redacted]

7. (U//~~FOUO~~) PUZZLES: Solution to KRYPTOS KRISTMAS KWIZ by [redacted]

8. (U) EDITORIAL CORNER

****
//

1. (U) PERSPECTIVE: "Changes"

(U//~~FOUO~~) Each issue of this newsletter features the perspective of a Senior on a CA topic of his/her choice. This issue we are pleased to feature the thoughts of [redacted] has been

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

a cryptanalyst for 25 years at the Agency.

(U) These articles are a great way to review the changes that have affected the Agency. With more and more people leaving, we are in danger of losing our history. That is not to say things were better in the past. In many ways the crypto community has never been stronger. However, I would like to review some of the tours I have had in my career and discuss some of the lessons they might suggest.

(U) One of the major changes in the Agency is size. When I arrived, a small group of people could control the entire community. When this small group made a decision, it held. Now power is so diffused, that managers will tell you they have control over little.

(S//SI) One of my best tours was in P12. Mr. Lutwiniak was the head, and his power and prestige can be measured by the fact that he was one of the two people that [redacted] feared. This was a virtual organization in that we did not work together, but were farmed out to organizations. This allowed you to take assignments that were interesting, but perhaps dangerous to your career. I spent some time in an engineering area and learned a lot about optical correlation. Even more importantly I learned a lot about how a research area interacts with operations. As the only mathematician, this was not a tour I would have chosen on my own. I went because I knew I had a powerful senior who agreed that this was an assignment that was good for the long run, even though it would not produce short-term results good for my career. It would be certainly possible to take such tours now. The difference is you would be much on your own. I had the luxury to know someone was watching and I could leave at a moment's notice. (b)(3)-P.L. 86-36

(U//FOUO) The other advantage to an organization like P12 is that a group of us could be sent to an organization that had an important problem,but was having trouble staffing it. It might be because the problem was very hard and discouragement had set in, or it might be a management problem. In any case we knew we were being sent with protection behind us. If it got really bad, we could always be pulled back. Since that was true, it was almost never necessary to request that. So on one hand we could be directed to problems that needed us, but on the other hand we retained the independence that every analyst wants. Today we have PODs, Expert conferences and more diversity tours than I ever thought possible. Do you ever get the sense that there is a plan behind any of this or that you are on your own? How often have you heard of a senior technical person being assigned anywhere?

(U//FOUO) I believe an organization like this would be a benefit to Z Group. I also believe that it probably cannot work. Who has the prestige to plan and protect careers like this? Would there really be support for some of these people to be taken out of organizations and be put under another's control. Thus you see that this is a management problem. You should also realize that when I talk about technical persons being "directed" to work on projects, I do not mean me. I mean everyone else. You want me to go where? Now just a second.....

(S//SI) Another assignment that I believe has some lessons was in the creation of [redacted] but it was exciting to be there at

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

the creation of an organization. The great lesson there was to immediately jump into the new technologies, even at the cost of short-term pain. The great advantage was that there was no legacy that had to continue. Thus the systems could be built at the present state of the art. Of course, this is not always possible. This is one of the hardest management decisions. There are always customers who are dependent on old systems. There is usually a long-term investment in older systems that cannot just be thrown away. However, I do believe we hold on too long to old methods and old technologies.

(~~C//SI~~) My latest assignment was in the [redacted] that became a part of [redacted]. Here again the fun was starting a new technology and a new area for Z Group. When we began, we assumed that we could learn from the experts in the field. We soon learned that the "experts" were those who were reading half a chapter in front of us. Thus we decided to just do it. We did our reading, took the courses, but especially started a project and got our hands dirty. At the start there was skepticism in other organizations about the ability of these Z Groupers. So we named ourselves TINE+ (The Incompetent NinE+ [redacted]) and produced a successful project that we then briefed to anyone who would listen. The lesson here again was that the way into a new technology is just to jump in and do it.

(b) (3)-P.L. 86-36

(~~S~~) The other thing I noticed was that engineers and cryppies looked at problems in different ways. It was important to integrate both ways of doing things. As a cryppie I always wanted to know everything about the problem. With modern communication we have a great filter problem. There is more information than anyone needs to know. We want to know enough to find and exploit weaknesses. So we should just learn what we need to know and ignore the rest. Easy to say! How do you determine what that is? You have to know enough about the workings of the system to be able to communicate with others working in the field. However, you can quickly find yourself involved in more and more details until it is hard to recall what the original problem was. It is very helpful in a team environment to be able to ask enough questions so that you can determine you really do not need to know more. The combination of teaming across disciplines and the efficient organization of information will be one of our major challenges.

(U//~~FOUO~~) Everyone tells us that we are entering a new world of communication. This is certainly true, but we should also remember that we are part of a great tradition of success and that our past history may have lessons for us in the future. In any case our golden years are still in the future.

"""""""

(U//~~FOUO~~) The Breakfast Affair for Newly Certified Cryptanalysts (BANCC) was held on 26 January, 1999 in the Canine Suite. In addition to a delicious buffet breakfast, the group was treated to some delightful words from [redacted] current President of KRYPTOS, [redacted] Chief Z, and [redacted] the Chairperson of the Cryptanalysis Career Panel.

3a. (U//~~FOUO~~) Text of [redacted] BANCC Speech

(b)(3)-P.L. 86-36

(U) I would like to commend the KRYPTOS Society for sponsoring this breakfast to honor our newly certified cryptanalysts. Those that we honor here today are the heirs to a world class tradition that has its modern roots in the successes of American and British cryptanalysts during World War II. The imagination, creativity and analytic rigor practiced by our predecessors have served as a model for every generation of cryptanalyst since.

(U) Those being recognized today have reached an important milestone in their careers--they have received formal recognition that they possess the skills to contribute to our future successes. By meeting the requirements of certification, they have shown a commitment to training and professional diversity--the foundations of our success over the years.

(~~S~~) There are many who would bury the art and science of cryptanalysis--it's too hard and manpower-intensive; the mathematics employed in the newer encryptions are better than our best computers; we can no longer rely on restrictions on strong encryption abroad; embedded encryption will preclude implementation errors... and on and on. It would be easy to agree, but only a few moments of thought bring to mind many such conversations over the years--every new technology was a threat; every new advance was the final straw that would drive us out of business. But each time, working cleverly and collegially, we have developed the tools that have taken us to a new level of achievement.

(~~S~~) It is these men and women we honor here today that must continue this tradition. Cryptanalysis can no longer be confined to decrypting point-to-point communications. We must broaden the scope to address the complete range of information security products which by encryption, compression, multiplexing or other advanced communication technologies serve to deny us straightforward access to communications of interest. Z Group today is profoundly different than the Z Group that was formed in 1992. By adding the [redacted] efforts to the cryptanalytic group, the corporation has recognized that the skills required to do signals analysis and [redacted] are similar to those practiced in the cryptanalysis group.

(b)(3)-P.L. 86-36

(U) Even in 1992, if I were giving a Z Group overview to a group from Capitol Hill, my theme would have been Z Group is more than you think. Cryptanalysts are more than you think. No matter what their job title, successful cryptanalysts think of themselves as problem solvers and have no preconceived notions of what it will take to solve the problems they are presented.

(b)(1)
(b)(3)-P.L. 86-36

(~~C//SI~~) Success may come from the standard bag of tools; success may be dependent on understanding the habits of the communicants; success may hinge on understanding the communications path; success may hinge on understanding the telecommunications environment; success may hinge on [redacted] success may be the result of reverse

(b)(3)-P.L. 86-36

[redacted]

engineering; success may be the result of sophisticated signals analysis, clever collection operations, discussions with TOPI analysts on target behavior; success may come from a combination of these factors; or success may come from just plain luck. A good cryptanalyst does not limit himself or herself to the bits on the screen. It is the totality of knowledge that leads ultimately to solution. And it is this willingness to do whatever is necessary that has carried us, and I believe will carry us to a successful future.

(U) It almost goes without saying that we must adjust our training paradigms to meet the accelerating pace of change in technology. The CA Panel is sponsoring several efforts to look at training and the way we currently deliver it. We hope to develop a model that takes advantage of commercial training packages for introductory knowledge and build on it by using in-house expertise to develop courses that give you an opportunity to apply your skills on real problems. We need you, our journeymen cryptanalysts, to work with us to identify and define the gaps. I encourage you to commit to being an active part of the CA community giving your time to serve on boards and committees that are formed to ensure that we do not get stale; that our skills remain world class; that we continue to be zealots about the need to stay on the leading edge of technology.

(U) It also should go without saying that we are challenged in ways today that are different than the past. We no longer have a monopoly on understanding cryptography. That Bruce Schnier's book on cryptography has become the reference of choice is but one example of the vast amount of knowledge that exists in industry and academia about our profession. The emerging global market is pushing industry to demand the export of strong cryptography to support their economic goals. Just 10 days ago, the New York Times featured an article entitled, "U.S. Officials Try to Sell Encryption Policy in Valley." The first two paragraphs of the article are instructive and summarize the challenge we face:

(U) "The Clinton Administration's campaign against exporting strong secret computer codes took to the road on Friday as the President's Export Council Subcommittee on Encryption held a meeting in Silicon Valley to try and build bridges between the computer industry and government."

(U) " Little harmony emerged, however, as the industry representatives turned a cold eye to the Administration's recent proposal and complained that increased foreign competition was in danger of surpassing American companies."

(S) So, it is no surprise to any of you that our challenges lie in advancing technology and now from the demands of the international marketplace. If the UCA Study is correct, we can expect the environment to be 80% encrypted by the year 2010. Today, [redacted] of our collection comes from encrypted communications. The evolution in communications that will occur in the next ten years must be tracked, piece by piece, change by change, by the men and women of the cryptanalytic community for success to continue.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U//FOUO) I challenge you whom we honor here today to identify and develop the opportunities that will emerge from the current landscape. Study the technology, study your targets, learn everything you can about the communications environment, form

(b)(3)-P.L. 86-36

[redacted]

alliances with your colleagues in related disciplines. Do not be content to "do your job." For in the end, the goal is not an academic one - the goal is to produce important and timely intelligence that provides information to military commanders and national policymakers. Yes, your job is to develop attacks, diagnose systems, write application programs, exploit cryptosystems, but never lose sight of the fact that you are the front line of defense for this nation. I welcome you into the ranks of professional cryptanalysts and urge you to use your intelligence and energy to continue the exceptional tradition of service to the nation that is the hallmark of the cryptanlaytic effort.

3b. (U) BANCC Newly Certified Cryptanalysts

(b)(3)-P.L. 86-36

(U//FOUO) Following those encouraging words, [redacted] newly certified Cryptanalysts were honored. [redacted] were present, while [redacted] are currently serving outside the U.S. When contacted with congratulations, the [redacted] non-attendees reported the following interesting tidbits:

(b)(3)-P.L. 86-36

(U//FOUO) The "GCHQ Chapter" of KRYPTOS also held a celebration for [redacted] newly certified cryptanalysts who is not currently stationed at NSAW. [redacted] reports that since she wasn't able to attend the BANCC in the Canine Suite, her new friends at [redacted] decided to have their own BANCC -- called the BAITUKFNCCWDWTFBHFSE (Breakfast Affair in the UK for Newly Certified Cryptanalysts Who Don't Want to Fly Back Home for Scrambled Eggs), complete with muffins, coffee cake, and a certificate suitable for framing!

(U//FOUO) [redacted] reported that she's jumped right in and gotten herself elected as Secretary of the CSE chapter of the KRYPTOS Society. Go [redacted]

(U//FOUO) The [redacted] newly certified Cryptanalysts include:

[redacted]

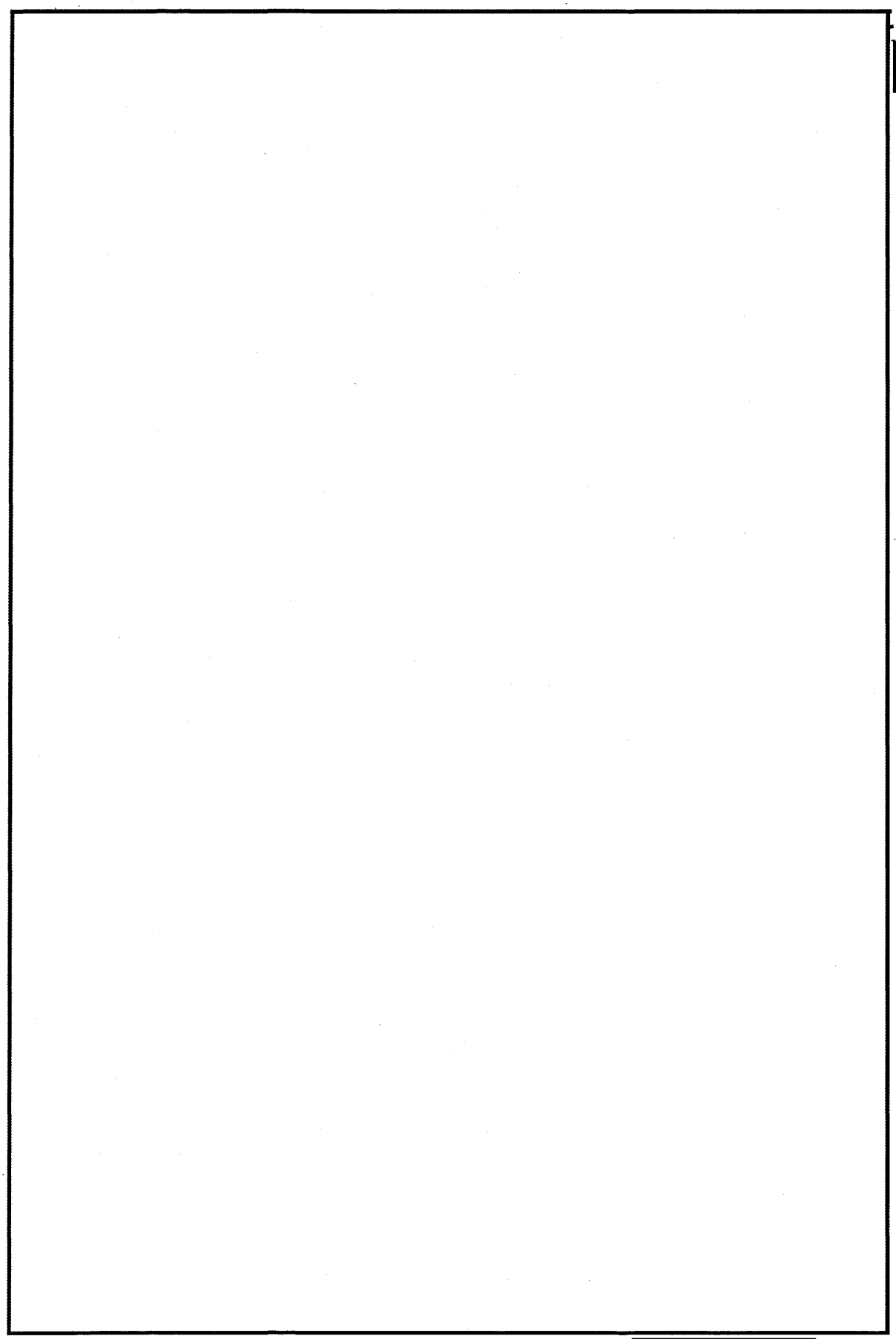
[redacted]

(b)(3)-P.L. 86-36
(b)(6)

[redacted]

(b)(3)-P.L. 86-36

[redacted]



(b)(3)-P.L. 86-36
(b)(6)

(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36
(b)(6)

[redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

[redacted]

4. (U) KRYPTOS SOCIETY NEWS

(U//~~FOUO~~) These are the 1999 KRYPTOS Society Officers:

President:
President-Elect:
Secretary:
Treasurer:
Member-At-Large:
Member-At-Large:

[redacted]

(b)(3)-P.L. 86-36

[redacted]

Member-At-Large:
Member-At-Large:

[redacted] (b)(3)-P.L. 86-36

5. (U) TECHNICAL HEALTH

5a. (C//SI) Understanding 56k Modem Technologies
by [redacted]

(U) Prior to the introduction of the new 56k-modem technologies, state-of-the-art modem transmissions over general switched telephone networks (GSTNs) were described in the International Telecommunication Union (ITU) Recommendations V.34 and V.34bis. These standards specify data rates up to 28.8 and 33.6 kbps, respectively. With the new 56k-technologies, modem transmissions over GTSNs can achieve data rates approaching 56 kbps in the downstream direction, although upstream speeds are still limited to the previous maximum data rates (28.8/33.6 kbps).

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

5b. (U) DO Technical Health Advisory Board Special Achievement Awards

(b)(3)-P.L. 86-36

[redacted]

(U) The DO Technical Health Advisory Board (THAB) recently announced the recipients of the DO Technical Health Special Achievement Awards. These awards were established to recognize special acts or achievements that have significantly advanced the technical health of the Operations Directorate and its ability to achieve mission goals.

(U) The key concept in the selection criteria for these awards is "enabling others," and each of the recipients either:

1) provided personnel with the right skills to accomplish the mission;
2) provided personnel with the right tools to accomplish the mission; and/or
3) provided the proper support infrastructure for the workforce to accomplish the mission

at a level of scope and impact appropriate for a Special Achievement Award.

(U) The Z Group recipients were notified of their awards by Scribner Messenger, Director of the DO THAB, on 14 September at a small ceremony in the Z Conference Room, and were formally recognized at a DO Technical Health Awards and Masters Ceremony on 5 November, 1998. Among this group of recipients were the following individuals:

(U//~~FOUO~~) [redacted] (Nominator: [redacted])

[redacted]

(b)(3)-P.L. 86-36

****

(U//~~FOUO~~) [redacted] (Nominator: [redacted])

(~~S//SI~~) [redacted] has developed programs, algorithms, and software which have had a significant impact across the Operations Directorate. His contributions include:

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

****

(U//~~FOUO~~) [redacted] (Nominator: [redacted])

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

****

(U//~~FOUO~~) [redacted] (Nominator: [redacted]

(C//SI) [redacted] has provided extensive signals analysis training, tools, and techniques to analysts in the Signal Development Center (SDC), which have enabled them to readily identify, analyze, and [redacted] extraordinary commitment to enhance the signals knowledge of others since he has done this as an adjunct to his primary job responsibilities.

(b) (3)-P.L. 86-36

****

(U//~~FOUO~~) [redacted] Z61 (Nominator: [redacted] Z61)

(C//SI) [redacted] completely rewrote the unclassified text for the NCS [redacted] on his own time. These updated course materials have resulted in current and viable courses, which can be maintained with minimal effort for years to come. After completing the revisions, he taught both a two-week and one-week version of the courses.

(b) (1)
(b) (3)-P.L. 86-36

---

6. (U) LETTER TO THE EDITOR

(U) To: _Tales of the KRYPT_ (TOTK) Editorial Board,

(U) Having read the latest TOTK, I just wanted to commend the newsletter staff for doing such a great job!

(U) Don't know if you are aware, but I won the contest for naming the newsletter, so I have always had a "proprietary" interest in it.

(U) I have to say that I expected it to do well, because I really had faith that the CA community was filled with talented and enthusiastic people. I felt that our career field was alive and well, and would remain that way, despite a lot of negativism at the time TOTK was created.

(U) The latest issue just convinces me again that my faith was warranted. Congratulations on doing such a nice job on "my" newsletter!

(U//~~FOUO~~) [redacted]
December 29, 1998

(b) (3)-P.L. 86-36

[redacted]

7. (U//~~FOUO~~) PUZZLES: Solution to KRYPTOS KRISTMAS KWIZ by [redacted] (b)(3)-P.L. 86-36

(U//~~FOUO~~) Long-awaited results from the 1998 Kryptos Kristmas Kwiz are here! First place goes to the team of [redacted] with an astounding score of 101! Other entries were provided by (in no particular order): [redacted]

(U) The official answers are below. Alternative answers were possible in many cases and bonus points were sometimes awarded. Total points possible, not including any bonus points, were 101.

1.Between BALL and LIGHT. There are 5 categories:

ELEMENTS	(Barium Meal, Carbon Copy, Copper Beech, Gold Standard, Iron Curtain, Lead Pencil, Neon Light, Oxygen Mask, Silver Lining, Tin Soldier)
ACTORS	(Bob Hope, Cary Grant, Clara Bow, Doris Day, Gregory Peck, John Candy, Lucille Ball, Mae West, Shirley Temple, Tom Cruise)
ANIMALS	(Catnap, Cowslip, Dogwood, Foxglove, Horseplay, Pig-Iron, Rabbit Punch, Sheep-dip, Tiger Lily, Wolf Whistle)
BEATLES SONGS	(Come Together, Day Tripper, Hello Goodbye, Get Back, Lady Madonna, No Reply, Nowhere Man, Paperback Writer, Rocky Raccoon, Yellow Submarine)
? of the ?	(Compliments Season, End Road, Run Mill, Salt Earth, Sign Cross, Six Best, Slip Tongue, Tip Iceberg, Turn Century, Wide Mark)

2.Between GRASS and IRISHMAN. Each entry clues a word, again in five sets:

PROGRESSIVE - ALMOST BLOWY CHIPS DEITY DIRTY FLOPS FORTY GHOST GLORY HORSY

EVEN (OR ODD!) - AEGIS CAMEO IMAGES MAGIC MICKEY QUACK QUEASY SQUEAK SMOKE SUCCESS

PALINDROMIC - DEED KAYAK LEVEL MARRAM MINIM PEEP REFER REDDER SAGAS TENET

MULTIPLE HOMOPHONES - BUY FOUR EIGHT HOLY NEW OAR RIGHT SITE TWO WEAR

MULTIPLE ANAGRAMS - DANGER EATS MERIT PLEATS PRIEST RACED SIREN SPARE STAR TRACE

3.(a) PROPANE (b) TRIGON (c) MARCH (d) O and ET

4.(a) TEAR (TREAT EATER REATA TERRA)
(b) STARE (STARES TREATS ASTARE RAREST TEASER)
(c) PADRES (DAPPERS PARADES PADDERS DRAPERS SPEARED SPREADS)

5.(a) 1189 (b) paper sizes (A0... A10) in millimeters (b)(3)-P.L. 86-36

[redacted]

6.(a) BINDER - splits into two German (French) words
(b) TRACTORS - middle letters anagram to a vegetable (fruit)
(Note - this was the intended answer, but the word TRACTORS was accidentally left off the actual puzzle, so the question was thrown out. A bonus point was awarded to anyone who came up with TELEGRAPHIC, with the justification being that other middles of words anagrammed to a fruit that grows on trees, this one on a vine.)

(c) HUNTERS - word formed by cyclic shift right (left)
(d) NECROMANCY - beginning (ending) sounds like part of the body
(e) ALLIANCE - even (odd) letters spell a word

7.(a) 143 (each number is one more than the sum of the previous two)
(b) 8 (lengths of words TO BE OR NOT TO BE THAT IS THE QUESTION)
(c) 6 (digits of pi, plus 1)
(d) 3 (lengths of Roman numerals, I II III IV V etc)
(e) 988 (prime factors sum to 36)

8.(a) STYLE (E at position 1, 2, 3, 4... rest are consonants)
(b) OPAQUE (first contains JKL, second KLM etc)
(c) UNQUESTIONED (middles spell out "TO BE OR NOT TO BE...)
(d) ACADEMICAL (words from first or second halves of alphabet; lengths increment)
(e) EVENTS (words contain letters ONE, TWO....)
(f) WHITLOW (written one under the other, diagonals, reading up, are WARRELL and WHORLOW)
(g) COMING (DO at position 6, RE at 5, MI at 4 etc)
(h) COAT (words result from adding a, b, c...)
(i) AIL (words can be preceded by a, b, c...to form other words)
(j) FLY (each word can be absorbed into the following word to produce another word)
(k) DETAINS (number of repeated letter between adjacent pairs of words is incremental)
(l) IN (each even word is formed by adding consecutive letter of the previous word, A=0, B=1 etc)
(m) UNNERVE (words begin with letter of German numbers EIN, ZWEI...)
(n) BEETLE (clues lead to CL, DJ, EG, FX, HQ, IT, MY, NB, OZ, PS, RA, UK leaving VW or WV)
(o) DEBILITATED (odd/even alternating, incremental lengths)
(p) VAIN (anagrams of first names, alternating male/female)
(q) PUMPKIN (each word contains an anagram of a colour, starting at position 3 or 4, alternating)

9.(a) MEMORIAL (b) MALARIA

10.8 4 (lengths of words "question" and "mark")

11.MARS (My first is in first [MERCURY] but not in seventh [URANUS], etc.)

12.(a) 334 (10 less than a square, the others are 10 more)
(b) 625 (Putting the first digit at the end gives a 4th power not a cube)
(c) 246 (Not a straight line on a numeric keypad)
(d) 555 (Not a straight line in the standard 3x3 magic square)

13.(a) ACT, ART, BARE, FLOW, GOD, HARKS, HEAR, LOIN, LOSE, LOW, SHORE, STAKE

(b)(3)-P.L. 86-36

(each word given is associated with an animal which anagrams to give the above)

(b) COURAGE, CROSS, DELIGHT, FLY, HEEL, HORN, MAN-OF-WAR, PASTRY, ROLL, ROULETTE, SHEPHERD, SUMMER/TEA, WALL/WHISPER (each CITY leads to the adjectival form of the country with which these words are connected)

(c) BLACK, BLUE, BROWN, GREEN, INDIGO, ORANGE, PINK, RED, SCARLET, WHITE, YELLOW (middle words are synonyms of given words, each associated with a colour)

(d) CHURCHMOUSE, COOT, CUCUMBER, DIE, DOORNAIL, FEATHER, FIDDLE, HATTER, KITE, PICTURE, RAKE (middle words are the opposite of the given words, and feature in similes together with the third words)

(e) BARREL, BLUE, BOBTAIL, CANDLE, CHARITY, HARRY, JUMP, MARY, MATCH, QUARTERED, SINKER (middle words rhyme with given words, QUARTERED, SINKER (middle words rhyme with given words, and are the first words of 3-word phrases, e.g. RAG TAG and BOBTAIL)

14. LADY GUESS PARTY ESTATE COLUMN SENSE HEAVEN (substitution is A=N, B=O C=P etc., giving (sixth) SENSE, (third) PARTY, (second-) GUESS, (seventh HEAVEN, (fourth) ESTATE, (first) LADY, (fifth) COLUMN

15. 14: DELTA JULIET HOTEL ECHO CHARLIE OSCAR SIERRA WHISKEY YANKEE NOVEMBER VICTOR UNIFORM ROMEO FOXTROT (other orders possible)

16. (a) A (b) L [el] (c) P [pea] (d) h (e) ALPH (f) sunless C [sea]

17. (a) each number is the product of the numerical equivalents of the letters in a country's name, A=1, B=2, etc., CHAD is 96 (3.8.1.4), CUBA is 126 (3.21.2.1), etc.

(b) 3024 is the value for both ALBANIA and CHINA.

(c) 12960 (CHILE & HAITI). [A few entries later, 17640 (ANGOLA & BENIN)].

18. MAGPIE (words enciphered by adding 1 for sorrow, 2 for joy, etc.)

19. DOTS AND DASHES.

20. ORGY and SEX. Using A=1 ... Z=26, in each word the letter N is the sum of (N-2) and (N-1) mod 26.

21. (32 6) 4 series of numbers progress position through the series (8 11) of matrices - integers, fibonacci, odds, powers of 2

22. a. 18 From KNIGHTS and THING, K + S = 5
From READS and ADORE, S - O = 2 thus K + O = 3
From HEARTY and RATE, H + Y = 3
From POLISH and SPOILS, S - H = 1 thus Y + S = 4
From PURPOSE and SOUP, P + R + E = 13
From ADORE and DARTS, E - T = 2 thus P + R + T = 11
Thus KRYPTOS = 3 + 4 + 11

b. 36 Y and O are both less than 3 so P must be 6, and this enables H, K, O, S, U and Y to be solved (2, 2, 1, 3, 2, 1 respectively), which in turn enables R + E (7), T + R (5), E + A (7), and T + I + N + G (17) to be solved.

(b)(3)-P.L. 86-36

23.(97,98) The last letter of the first number and the first letter of the second number are the same. These are all the 2-digit examples.

24.(a) NE (series 1, 3, 6, 10, 15 ... substituting DECRYPTION for 0123456789
(b) bCs (series n**3 for incremental n, substituting ACFJOUbjs, the positions of these letters being 1, 3, 6, 10, 15 , etc. in the alphabet)

25.MEGA. The table contains the names of the 24 letters of the Greek Greek alphabet in order through the rows.

26.GOBBLEDYGOOK. The top row of the typewriter is shifted by one position in the second line, then the second row in the third line, then the bottom row in the last line.

27.BLACKSMITH and GUNPOWDER

28.RUDYARD KIPLING (FARE = PASSENGER, FOOD; FAKE = DOCTOR, COOK: TUCK = CRAM, FOLD; TICK = CREDIT, BEAT : DULL = DIM, BLUNT; PULL = DRAW, STRETCH: WILY = ASTUTE, CRAFTY; WILL = COMMAND, WISH: BLAND = DULL, MILD; BLIND = IGNORANT, OBSCURE: FIRE = IGNITE, ENTHUSIASM; FINE = PURIFY, SUBTLE: DANDER = PASSION, ANGER; DANGER = HAZARD, INSECURITY)

29.(a) CHARLIE CHAPLIN (b) ABRAHAM LINCOLN (c) MARGARET THATCHER

30.CHRISTMAS. Deleting the first and third letter of each group gives MERRY CHRISTMAS AND A HAPPY NEW YEAR.

"""""""

~~SECRET//COMINT//X1~~

Derived from: Multiple Sources
24 February, 1998
Declassify on X1

DERIVED FROM: NSA/CSSM 123-2,
DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR"
DATE OF SOURCE: 3 SEP 1991

~~SECRET//COMINT~~

(b)(3)-P.L. 86-36

(b) (3)-P.L. 86-36

SECRET//COMINT

(S) POC:

(U) *Last Modified: 10/30/2002 11:42:24*

(U) PE EXTERNAL PAGE

SECRET//COMINT-SPOKE//XI

****
* TALES OF THE KRYPT *
****

March - April 1999

//
****

++
//

(U) TABLE OF CONTENTS:

1. (U//FOUO) PERSPECTIVE: "Thoughts," by Ann Caracristi

2. (U) CALENDAR OF EVENTS

3. (U) CRYPTANALYSIS CAREER PANEL NEWS: New Skills Field Director

4. (U//FOUO) COMMUNITY NEWS: "Women in Z," by [redacted]

5. (U) TECHNICAL HEALTH

5a. [redacted]

5b. (U//FOUO) "Navajo Code Talkers," by [redacted]

6. (U//FOUO) PUZZLES: "Thank You to Former _Tales of the KRYPT_ Puzzle Editor [redacted]

7. (U) EDITORIAL CORNER

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

****
//

1. (U) PERSPECTIVE: "Thoughts"

(U//FOUO) Each issue of this newsletter features the perspective of a Senior on a CA topic of his/her choice. This issue we are pleased to feature the thoughts of Ms. Ann Caracristi, former D/DIRNSA.

(U//FOUO) Recently I was invited to serve on a special Cryptanalytic/ Cryptomathematics Panel of the NSA Scientific Advisory Board (NSASAB), and I was excited at the prospect of being able to learn about today's problems from the current generation of cryptanalysts and research mathematicians. I was looking forward to hearing their candid views. And I was sure the views would be candid because I had "grown up" listening to and learning from some of the NSA "math mafia's" most distinguished practitioners. The first of these was Dr. Solomon Kullback ("Kully"), who was certainly responsible for whatever modest success I had as a young cryptanalyst long ago; but the list covers all the years of my NSA life. It includes especially those mathematicians associated with what used to be known as the "A Group" problem. There was Dick Liebler, Arthur Levenson, Phil Dibben, Peter Jenks, and Bob Highbarger, Jim Bates--and a host of others. Equally candid were those distinguished cryptanalysts who, without advanced degrees in mathematics, nevertheless made such vitally important contributions to our successes. Bill Lutwiniak and Frank Raven are two of the "legends" who first come to mind.

(U//FOUO) But, frankly, I was somewhat intimidated by the fact that I

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

(b) (3)-P.L. 86-36

9/24/2010

was the only non-mathematician on this NSASAB panel, and I wasn't sure that I could even be a qualified "listener." What to do? Well, I had just read a review of the _Man Who Loved Only Numbers_, so I got a copy of that book by Paul Hoffman and discovered that it was not only a highly readable tale about the eccentric Paul Erdos but a touching account of the wonderful support Erdos received from our own NSASAB member [redacted]. Furthermore, the author was able to make understandable many of the mathematical theorems and problems, which so captivated Erdos and his colleagues. This, then, led me to read Simon Singh's _Fermat's Enigma_, the story of the long search for a solution and how Andrew Wiles finally produced the proof of Fermat's last theorem. Again, mercifully, the author wrote with great clarity about very complex concepts. So, I was armed with that most deadly of all weapons: a little knowledge.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Actually, of course, mathematicians usually are very skilled at communicating their ideas--in the shorthand of their peers where appropriate and in the language of the layman when necessary. Being on the panel made me think again about why I have always enjoyed so much the company of these people who have always been the backbone of our business. In the past, I'm sure, I was delighted by the pure originality and eccentricity of so many of the "characters" who played important roles in solving the "impossible" problems. But, of course, bright people are always fun to be around. What is so special about the "cryptos" (mathematicians and analysts)? I suspect it is that they are trained to be forthright and fearless in dealing with the problems at hand. They don't equivocate. Two plus two is four. Not ALMOST four. On the other hand, they know that there are still mysteries to be uncovered. What is the largest prime? How is the key generated? They are receptive to new ideas and concepts. They are optimists. We know how tenacious a cryptanalyst must be and how important it is to have confidence in the validity of an attack. And, although they can be fiercely competitive, mathematicians have a habit of (maybe even a compulsion for) sharing and defending their ideas. And finally, these are people who frequently retain a charming touch of childlike wonder and appreciation for both the elegant and the absurd. (It's not surprising that the author of _Alice in Wonderland_ was a mathematician. It could as well have been a cryptanalyst.)

(U) In the course of our deliberations, which included discussions with principals from Z and K and with a cross-section of people who entered the cryptologic field through the various outreach programs, through the Cryptologic Mathematician Program (CMP), and by way of the Cryptanalytic Career Panel, we were much impressed by the quality and enthusiasm of the participants. We were encouraged to find that CMP'ers are being exposed to a widening variety of problems throughout the organization. They are demonstrating that advanced math techniques can play a vital role in solving some of our new collection and data selection challenges. I, personally, was pleased to learn that there was still a demand for non-mathematician cryptanalysts. Graduates of the CA Career Panel program are much respected; however, current hiring priorities do not allow us to recruit potential cryptanalysts from outside of the mathematics discipline. That is a disappointment.

(U) It is probably not surprising to the readers of _Tales of the KRYPT_ that we came away in admiration of the ingenuity continually being demonstrated in the battle against the incredibly hard problems which the Agency faces today. Our strategy, however, must be directed towards the future and that means we cannot rest. Concerned that the Agency might falter in its commitment to a robust CMP hiring effort, we argued strongly in support of that and other related programs.

(U//~~FOUO~~) As a final personal observation, I was amazed at the success and popularity of the technical track--pleased to see how well George Cotter and others had brought into being what was only a "glint in the eye" when I retired in 1982. However, I was somewhat disturbed to hear that its very success discourages many of the most talented of our young analysts and cryptomathematicians from taking on the challenge of management positions. I firmly believe that if they want to ensure the health and vitality of the NSA of tomorrow, the cryptanalysts and mathematicians of today must be willing to accept the responsibilities of leadership when

(b)(3)-P.L. 86-36

[redacted]

opportunities arise.

---

2. (U) CALENDAR OF EVENTS

(U) PLAN AHEAD

Jul 31 (U) 7:05 PM, KRYPTOS/CMI Night at the Bowie Baysox.

---

3. (U) CRYPTANALYSIS CAREER PANEL NEWS: New Skills Field Director

(U//FOUO) The CA Community welcomes [redacted] as the new DO Skill Field Director for Cryptanalysis, replacing [redacted]

(b)(3)-P.L. 86-36

---

4. (U//FOUO) COMMUNITY NEWS: "Women in Z," by [redacted]

(U) March 1999 was Women's History Month. These are some statistics on the [redacted] women currently assigned to Z Group.

(U) We have a lot of women who have various certifications and several have more than 1. Here is a breakdown of how many women in Z are certified in a particular field:

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

(U) There are several women assigned to technical programs. [redacted] women are in the Senior Technical Development Program and [redacted] woman is in the Senior Leadership Development Program. We have [redacted] women who are flag badgers. [redacted] have associate degrees, [redacted] have bachelors degrees, [redacted] have masters degrees and [redacted] have doctorate degrees. [redacted] are assigned are assigned as Chiefs at Office and Division levels and [redacted] are Chiefs at the Work Center level. Women in Z have also taken various field assignments.

(b)(3)-P.L. 86-36

5. (U) TECHNICAL HEALTH

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

(U//FOUO) For more information about Z215, please see our web pages at [redacted] or contact our managers, [redacted]

5b. (U//FOUO) Navajo Code Talkers, by [redacted]

(U) As I was passing through the Navajo Reservation in northeastern Arizona recently, I stumbled on a display about the Navajo Code Talkers during World War II (WW II) at the Burger King in Tuba. Although they had Japanese and American fatigues and various paraphernalia on display, the information contained in a local newspaper article about the origins of the group was the most interesting.

(U) At the start of the U.S. participation in WW II, thousands of suggestions were sent to the War Department from citizens. Among them was a suggestion from a low-ranking officer, the son of a former missionary to the Navajo, that the Navajo could provide secure communications in their native language. Eventually the officer convinced his commander to let him test the idea. The Navajo he recruited for the trial run were so successful that a major recruitment effort was undertaken.

(U) Many of the Navajo recruits had never been off the reservation previously. They served in the Pacific Theater and were crucial to the success of a number of battles. The code they developed using plaintext Navajo words was so good that it was never broken. In fact, Navajo who were not privy to the development of the code could not understand it--they said the words were right, but they made no sense.

(U) On one occasion, a Navajo had trouble convincing friendly troops that he was not an enemy spy who should be shot. (Fortunately, he eventually persuaded them.) Thereafter, each Navajo Code Talker was paired with a Caucasian soldier who could vouch for him if the need arose.

(U) Also on display at the Burger King was a certificate signed by President Ronald Reagan acknowledging the contributions of the Navajo Code Talkers. (Their existence had remained classified for decades after the end of World War II in case the country needed their services again in some future conflict.)

(U) I have since heard that other Native American tribes, including the Sioux, performed a similar function during World War II.

(b)(3)-P.L. 86-36

---

6. (U//FOUO) PUZZLES: Thank You to Former _Tales of the KRYPT_ Puzzle Editor [redacted]

(U//FOUO) Since 1995, [redacted] has provided what may be the most popular regular feature of _Tales of the KRYPT_ (TOTK): the puzzle! Usually, [redacted] was prompt to a fault turning in the solution to the previous issue and the new puzzle for the current issue, but there was one occasion when I had the issue just about ready except I didn't have Robert's input yet. I put out a draft just for proofreading and raised a storm of protests: "How dare I even consider publishing without Robert's puzzle?" Needless to say, that issue did have the puzzle by the time I published it!

(U//FOUO) Robert provided close to 50 puzzles in his 4 years contributing to TOTK. The only break he had was in the December issue each year, when our GCHQ friends [redacted] provided the annual "KRYPTOS KRISTMAS KWIZ." But even then, Robert was the conduit for providing the puzzle and its solution, and for keeping track of answers coming in from prospective solvers, so he was still responsible for puzzle work.

(U//FOUO) Because many are daunted by the prospect of signing up to regularly providing a sufficiently intriguing puzzle issue after

(b)(3)-P.L. 86-36

[redacted]

issue, finding a single individual to replace Robert has proved impossible. However, TOTK Assistant Editor [redacted] gently persuaded a team of three intellectually curious individuals to commit to providing a puzzle for each issue. So beginning with the next issue, [redacted] will be our Puzzle Editors. Please send them your puzzle contributions: [redacted]

(U//FOUO) [redacted] we can't thank you enough for making our occasional breaks from work intellectually fun. May your puzzles be the most tedious work you ever have to perform!

***

~~SECRET//COMINT~~

(~~S~~) POC: [redacted] info
(U) *Last Modified: 10/30/2002 11:42:24*
(U) PE EXTERNAL PAGE

~~SECRET//X1~~

****
* TALES OF THE KRYPT *
****
May - June 1999

//
****

++
//

(U) TABLE OF CONTENTS:

1. (U//~~FOUO~~) Perspective: "The More Things Change, the More They Stay the Same"
by [redacted] (b)(3)-P.L. 86-36

2. (U) Calendar of Events

3. (U//~~FOUO~~) Cryptanalysis Career Panel (CACP) Personnel Changes
by [redacted] Assistant Executive, CACP

4. (U) KRYPTOS Society News

4a. (U) Nomination Call for KRYPTOS Society Distinguished Members

4b. (U) KRYPTOS Society: Call for Literature Contest Papers

4c. (U) Annual Peter Jenks Community Service Award: Call for for Nominations

4d. (U) Annual Norman Roberts Award: Call for Nominations

4e. (U) Second Annual TECHNICAL TALK Contest

5. (U//~~FOUO~~) Technical Articles
Julie on Math: "Where are all the Transcendental Numbers?"
by [redacted] AMP Intern (b)(3)-P.L. 86-36

6. (U//~~FOUO~~) Puzzles: "How Many Children?"
by [redacted]

7. (U) Editorial Corner

""
//

1. (U//~~FOUO~~) PERSPECTIVE: "The More Things Change, the More They Stay the Same"
by [redacted]

(U//~~FOUO~~) Each issue of this newsletter features the perspective of a Senior on a CA topic of his/her choice. This issue we are pleased to feature the thoughts of [redacted] has been a cryptomathematician for 21 years at the Agency.

(U//~~FOUO~~) I began my Agency career in 1978 working for [redacted] on the [redacted] This was a diagnostic problem which had been around for a number of years and involved a lot of data and a large number of people. I then spent three years at GCHQ and one year in B63, before joining the [redacted] where I have been ever since. (b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

(U//~~FOUO~~) One of the things I remember from my first year at NSA was a CryptoMathematics Institute (CMI) talk given by [redacted]. This wasn't a technical talk, but rather a discussion of the future of cryptanalysis. I didn't have much perspective, but it was clear that Mike was trying to rebut the apparently widespread conviction that the tremendously rapid changes in technology and 'outside' sophistication in subjects cryptographic were quickly bringing the era of NSA effectiveness to an end. His theme was that, on the contrary, the new technologies presented unprecedented new opportunities. He predicted that this technology would increase the amount of communications available to us, and would result in NSA maintaining a position of importance in the U.S. Intelligence Community. Of course, twenty years after this we can see that his view was probably a bit pessimistic. NSA has done better than any of our futurologists thought possible.

(b) (6)

(U//~~FOUO~~) Again today the commonly accepted wisdom seems to be that the tremendously rapid changes in technology and 'outside' sophistication in subjects cryptographic are quickly bringing the era of NSA effectiveness to an end. I don't believe it. I think that the same set of arguments advanced by [redacted] twenty years ago are still valid. The new communications technologies have made communications easier for all of our targets. These targets are going to use this opportunity to increase their communications, and our opportunities as well. All of the systems in use are designed, implemented, maintained, and operated by human beings. This means that mistakes are inevitable. As a friend once remarked, "You can't build an idiot-proof system because they keep coming up with better idiots."

(~~C//SI~~) Just as it was in 1978, the problem for NSA is not a lack of opportunity, it is finding and taking advantage of the new opportunities being presented to us. This is a considerable challenge, but not one that is appreciably more difficult than the ones that we have surmounted in the recent past. We have had to

[redacted]

(b) (1)
(b) (3)-P.L. 86-36

there is no reason that these problems cannot be overcome, or skirted around, as have the problems of the past.

(U//~~FOUO~~) I don't believe that we are going through a "hard right turn", or that we need to do so. In fact, as I look around I feel that our jobs as cryptanalysts have not really changed all that much. We are still expected to make sense of observed non-random phenomena. The foci of our efforts have changed, but the intellectual processes we use are not substantially different from those our precedessors used to solve their problems. It is certainly true that we need a different knowledge base than analysts of twenty years ago, but they also needed different knowledge than their predecessors. Analysts have always needed to continue learning and expanding their knowledge to keep up with the changing cryptographic environment.

(U//~~FOUO~~) Even as we shift our attention and resources to new technologies, Z Group is presented with problems that seem to come out of the past. There are several [redacted] problems which feel very much like [redacted] did. For instance, I am now working on [redacted]

[redacted]

(b) (3)-P.L. 86-36

****
//////////

2. (U) CALENDAR OF EVENTS

Jun 25 (U) Deadline for Nominations for KRYPTOS Society Distinguished Members
(See article 4a.)

[redacted]

(U) PLAN AHEAD

(b) (1)
(b) (3)-P.L. 86-36

Jul 8 (S//SI) KRYPTOS Society Talk: An Overview of [redacted]
by [redacted]
0930 in the Friedman Auditorium

(b) (3)-P.L. 86-36

Jul 30 (U) Deadline for Nominations for the KRYPTOS Society Literature Contest
(See article 4b.)

Jul 31 (U) 7:05 PM, KRYPTOS/CMI Night at the Bowie Baysox

Jul 31 (U) Deadline for Nominations for the PeterJ enks Community Service Award
(See article 4c.)

Jun 31 (U) Deadline for Nominations for the Norman Roberts Award
(See article 4d.)

Jun 31 (U) Deadline for Nominations for KRYPTOS Society Technical Talk Contest
(See article 4e.)

****
//////////

3. (U//FOUO) Cryptanalysis Career Panel (CACP) Personnel Changes
by [redacted] Assistant Executive, CACP

(U) CACP Certification and Personnel Changes

(U//FOUO) Congratulations to [redacted] on certification as cryptanalysts!

(b) (3)-P.L. 86-36

(U//FOUO) The CACP welcomes the following:

[redacted] as Chairman of the CA Technical Track Review Panel,

as a Member of the CA Technical Paper Review, and

and [redacted] as Members of the CA Technical Program Review.

****
//////////

4. (U) KRYPTOS Society News

4a. (U) Nomination Call for KRYPTOS Society Distinguished Members

(b) (3)-P.L. 86-36

(U) Each year the KRYPTOS Society selects retired individuals as Distinguished Members of our organization to honor them for their contributions to the field of Cryptanalysis (and CA-related disciplines). The individuals selected in the past have been known for their technical accomplishments or management of cryptanalytic endeavors.

(U//FOUO) We invite you to provide the Nominating Committee [redacted] with names for consideration. Please include your reasons for your suggestions.

(U) Following are some guidelines which the Nominating Committee will use:

(U) 1. In selecting individuals for distinguished membership, KRYPTOS strives to honor recent retirees or sterling figures from the past who have made their mark in some way on the cryptanalytic community.

[redacted]

(U) 2. Because the KRYPTOS Society was founded to further the interests of cryptanalysis, emphasis should be placed primarily on cryptanalytic work done by the individual, but with consideration also given to cryptomathematics and cryptoprogramming contributions.

(U) 3. The individuals should have had actual hands-on experience in CA during a major portion of their careers. Cryptanalytic management experience, to the extent that the individual demonstrated dedication to the advancement of cryptanalysis, should also be considered.

(U//~~FOUO~~) Previously selected Distinguished Members are listed on the NSA WEB: [redacted]

(U//~~FOUO~~) Names should be forwarded to [redacted] by 25 June 1998. Please use "KRYPTOS Distinguished Members" as the Subject line of your email.

4b. (U) KRYPTOS Society: Call for Literature Contest Papers

(U) The annual KRYPTOS Society Cryptanalytic Literature Competition is now underway. The competition is open to all personnel at NSA, GCHQ, CSE, DSD and GCSB, to personnel on field assignments, and to retirees (consistent with security considerations).

(b)(3)-P.L. 86-36

(U//~~FOUO~~) The papers may treat any topic in the broad category of professional cryptanalytic literature, including:

- _____operational cryptanalytic problems, either SIGINT or INFOSEC;
- _____cryptanalytic research;
- _____history of cryptanalysis;
- _____topics not of a direct cryptanalytic nature but clearly relating to cryptanalysis, e.g. computer support of a cryptanalytic problem or communication trends relating to cryptanalysis.

(U) The judges will consider the following criteria:

- _____Is the paper an original discussion of a cryptanalytic subject? The paper should be a description of new work done by the author(s) or a survey of previous work giving proper credit.
- _____Is the paper well-written? Is the subject presented well? Is there a professional level of authorship, i.e. style, grammar, spelling, format, and credit?
- _____Does the paper constitute an important addition to the body of professional cryptanalytic literature?

(U//~~FOUO~~) Submissions may be written specifically for the competition. Papers written between July 1, 1998 and June 30, 1999 are eligible. Since the purpose of the competition is to expand the knowledge of members of the cryptanalytic workforce by making available papers on methods and problems which otherwise might not receive wide distribution, it is strongly recommended that entries carry a classification no higher than TSC. However, papers classified [redacted] will be accepted as will papers classified [redacted] Papers must be releaseable to USA/AUS/CAN/GBR/NZL.

(U) Cash prizes totalling $300 will be awarded to first, second, and third place winners at the discretion of the judges. The judges may also deem a paper(s) worthy of honorable mention.

(U) Anyone can enter a paper with the permission of the author. Neither the author nor submitter (if different) has to be a member of the KRYPTOS Society.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) If you have any questions regarding this contest, please contact [redacted]

(U//~~FOUO~~) To enter, please submit six copies of your paper to [redacted] by July 30, 1999. Each copy should be submitted with two cover sheets: the name(s) and organization(s)

[redacted]

of the author(s) and title on one sheet, and only the title on the other to facilitate impartial judging. The competition results will be announced at the KRYPTOS Society fall luncheon in October 1999.

4c. (U) Annual Peter Jenks Community Service Award: Call for Nominations

(U) Peter Jenks was the Founding Father of the Cryptanalysis Career Panel and the Founder of the Cryptanalysis Intern Program. In recognition of Peter Jenks' dedication to the field of Cryptanalysis, the KRYPTOS Society established the Peter Jenks Community Service Award. This award may be presented annually to an individual in recognition of exceptional service and contribution to the CA community.

(U) Eligibility

(U) Potential award recipients include NSA/CSS civilian employees and military assignees who are active in the CA community.

(U) Selection Criteria

(U) The President of the KRYPTOS Council and the Chairman of the Cryptanalysis Career Panel are responsible for providing the guidelines for recommending individuals for this award. The following basic selection criteria also apply:

(U) - The service and contribution must be in the field of cryptanalysis and reflect efforts which exceed those expected in the performance of the job.

(U) - Such endeavors may include, but are not limited to, service on the CACP, as a KRYPTOS officer, as a member of a CA TTRP, or as a judge for an award or contest. Further examples may include designing and teaching a new CA course, coordinating technical talks, or other efforts which serve the cryptanalysis community as a whole.

(U) Recommending Officials

(U//~~FOUO~~) Any individual or group of individuals may nominate/ recommend someone for this award. Such nominations, detailing the contributions the individual has made to the CA community, should be forwarded to the Secretary of the KRYPTOS Council, [redacted] (b)(3)-P.L. 86-36 by 31 July 1999.

(U) Procedures

(U) This award may be given annually, but there may be one or more years in which the award is not given. A certificate of Honorable Mention may also be awarded, at the discretion of the Council. Such awards will be made at the Annual KRYPTOS luncheon.

4d. (U) Annual Norman Roberts Award: Call for Nominations

(U) In recognition of Norman Roberts' talent for nurturing the skills of junior cryptanalysts, the KRYPTOS Society established the Norman Roberts Award in 1991. The award is presented annually to a junior analyst who has made an outstanding cryptanalytic contribution.

(U) Norman joined GCHQ in 1975 and won the respect and admiration of his colleagues for his innovative ideas and particularly for his ability to train and inspire younger analysts up to his untimely death in July 1990.

(U) Any KRYPTOS Society member may nominate any employee of CSE, DSD, GCHQ, GCSB or NSA who has made an outstanding contribution to cryptanalysis or a related discipline and who has worked in the cryptanalytic field for less than five years as of 31 July 1999. (For a nominee with more than five years' experience the citation

(b)(3)-P.L. 86-36

[redacted]

should explicitly draw the judges' attention to that fact and explain why the nomination should be considered as falling within the purpose of the Norman Roberts Award.)

(U) The citation must include an account of the work which attracted the nomination, specifying the individual contribution made by the nominee. It should include the names of the proposer and the nominee, who does not have to be a KRYPTOS Society member. Integrees will be regarded as members of their host Agency.

(U//~~FOUO~~) The winner's citation will be published to the membership so a citation should not exceed the TOP SECRET CODEWORD level; a compartmented annex may be provided. Nominations are due by 31 July, 1999 and should be mailed to the KRYPTOS Society Secretary, [redacted]

(U) The winner, selected by a joint UK/US panel, will be announced in October and presented with an engraved plaque. His/her name will be inscribed upon shields at CCHQ and NSA which list all winners.

(b)(3)-P.L. 86-36

4e. (U) The KRYPTOS Society Second Annual Technical Talk Contest: Call for Nominations

(U//~~FOUO~~) The second annual Technical Talk competition seeks to recognize the best technical presentation on a subject relating to cryptanalysis or one of its related disciplines. The contest is open to all personnel at NSA, GCHQ, CSE, DSD, GCSB, to personnel on field assignment, and to retirees (consistent with security considerations).

(U//~~FOUO~~) Talks presented in the timeframe 1 July 1998 to 30 June, 1999 are eligible for the competition. All recorded KRYPTOS talks given in that timeframe will be automatically considered (with presenters' permission). All talks must be videotaped and last at least 30 minutes. It is strongly recommended that entries carry a classification no higher than TSC. However, talks at the [redacted] and [redacted] levels will be accepted.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) The judging panel will consist of three judges from NSA and one judge from GCHQ. The winners will be announced at the annual Fall KRYPTOS luncheon and monetary prizes will be awarded.

(U) The judges will consider the following criteria:

(U) _____Is the talk an original discussion of a cryptanalytic subject? The talk should be a description of new work done by the presenter(s) or a survey of previous work giving proper credit.

(U) _____Is the talk presented in a manner which makes it easy to follow and understand? Is there a rapport between the speaker and the audience? Does the speaker demonstrate enthusiasm for the subject matter?

(U) _____Does the talk successfully serve as a vehicle for disseminating information about a relevant topic from the body of professional cryptanalytic knowledge?

(U//~~FOUO~~) Anyone can enter a videotaped talk with the permission of the presenter(s). Neither the author nor the submitter (if has to be a member of the KRYPTOS Society. If you have any questions regarding this competition, please contact [redacted]

(b)(3)-P.L. 86-36

(U//~~FOUO~~) To enter, please submit two copies of the videotaped talk, or indicate that the talk is available on videotape in the Z Technical Library, R51 Library, or another similar repository, to:

[redacted] or [redacted]

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

by July 31, 1999. Each entry should be accompanied by the following information: name and current organization of the presenter, title of talk, and classification of talk.

---

5. (U//FOUO) TECHNICAL ARTICLES
Julie on Math: "Where are all the Transcendental Numbers?"
by [redacted] AMP Intern

(U) This is a column in praise of pi, although it will be a while before she makes her grand entrance. (b)(3)-P.L. 86-36

(U) First, a review of the definition of "transcendental". Let us create numbers. The easiest numbers to create, the first numbers that ever get into a child's head, are the numbers that count things: 10 fingers, 2 eyes, 4 legs on a dog, 5 blue blocks, 3 red blocks, and so on. These are the most basic numbers there are. Counting things leads to adding things leads to subtracting things, until we have all the integers.

(U) Integers are not enough. Besides whole things, I might someday want to examine partial things. So let us invent integer fractions (fractions with integers in the numerator and the denominator). Split a cup into two pieces and measure 1/2 a cup of milk. Examining a person who is between five and six feet, I split a foot into 12 pieces and measure that she is 5 and 5/12 feet tall. Fractions can be awkward to handle, so we mostly use powers of ten in the denominator when we measure things and write the numbers in decimal form.

(U) I don't lose any numbers by only liking decimals because all fractions can be written as decimals. Any integer fraction--such numbers are usually referred to as rational numbers--converts either to a decimal with a finite number of decimal places or a decimal which eventually goes into a state of endlessly repeating a pattern (such as 1/3=.33333333.... or 1/2200=.00045454545454545...). The integers themselves are rational numbers since they are fractions with a denominator of 1 (decimals with nothing to the right of the decimal point).

(U) I now have lots of numbers. I have enough numbers to measure anything at all. I could measure a box and get 1 meter. Then I could divide the ruler into 10 pieces and get 1.5 meters. Divide into 10 again and I could get 1.56. Again, and 1.562, and at this point I would stop because my eyes can't distinguish 1.562 from 1.561 or 1.563.

(U) However, I want even more numbers. Moving up in complexity, I could run into the problem of needing to find numbers that are roots of polynomials with rational coefficients. For example, consider the polynomial (x^2)-5 (that's x squared minus five). Suppose I want to solve it. It seems like I should be able to solve it. I can make an increasing sequence of numbers whose squares are all less than five: 1, 2, 2.2, 2.23, 2.236, 2.23606, ... I can make a decreasing sequence of numbers whose squares are more than 5: 4, 3, 2.5, 2.25, 2.239, 2.23609... Somewhere in those sequences I should be able to capture a number which exactly solves x^2-5, a number which starts out 2.2360... However, there is no rational number (no finite or repeating decimal) whose square is 5. So let's invent all the numbers which are roots of polynomials with rational coefficients: these are referred to as algebraic numbers. All rational numbers are algebraic, since for example the number 1/3 is the root of both x-1/3 and 3x-1, the number 32.456 is the root of x-32.456, the number .00071 is the root of x-.00071, and so on. Also, it turns out that adding, subtracting, multiplying, or dividing algebraic numbers just gives more algebraic numbers.

(U) Here is where transcendental numbers come in. A transcendental number is any number that isn't algebraic. Could there be such numbers? The algebraic numbers consist of just about every number

(b)(3)-P.L. 86-36

[redacted]

you'll ever run into. How many numbers could I have possibly left out?

(U) According to mathematical logic, not only do transcendental numbers exist, but there are more transcendentals then there are algebraics. Lots more. So many more that, if you picked a random real number and it turned out to be algebraic instead of transcendental, you should be shocked.

(U) Let's give an example of being shocked. Suppose you measured the exact temperature of your room (with the magical completely accurate scientific thermometer that goes out to all decimal places) and the temperature turned out to be an exact whole number, such as 65.00000000000000000. That would be very surprising. You would think, why in the world would I get 65.000000000000000000000 instead of some messy fraction such as 65.000235236302116780000? This thermometer is broken.

(U) However, you would be wrong to think that a whole number is startling but a messy fraction is expected. The difference between transcendentals and algebraics dwarfs the difference between whole numbers and fractions. 65.000235236302116780000 is just as shocking as 65.000000000000000000000. Any algrebraic number, in particular any number with a finite number of decimal places, is impossibly unexpected. What you should expect to get is a transcendental number.

(U) That is the conclusion that mathematical logic gives, but it doesn't agree with my personal experience. If transcendental numbers are so common, then where are they? I've seen a lot of numbers in my life, and hardly any of them have ever been transcendental. When I measure a temperature, or take the length of something, or calculate a probability, I get an algebraic number.

(U) I think transcendental numbers are impossible to find because human beings are just not built to perceive them. We are constrained by the physical universe: It makes no sense to talk about measuring a number with an infinite number of decimal places. Above, I said that if you examined room temperature with a thermometer that went out an infinite number of decimal places, then you would see that it is transcendental. That statement did not actually make sense. It doesn't make sense to talk about measuring temperature to a hundred decimal places, much less an infinite amount. Once it's gone beyond several decimal places, then the level of precision the thermometer needs is so exact that it's at the subatomic level. What does temperature mean on the subatomic level?

(U) As another example, suppose I picked a board of wood. I chose it at random, so its length should be transcendental. But what does length mean once I go past a few decimal places and am at the subatomic level? For one thing, wood is made out of atoms, which are discrete. Also, atoms shift around all the time and have weird wave-particle duality. Measurement doesn't make sense on such a small scale.

(U) So, experiencing the universe through our physical selves, we will only measure rational numbers (basically, numbers with a finite amount of decimal places). By use of mathematical equations, we can manipulate rationals so that we produce algebraic numbers, but that's it. Transcendental numbers exist, but we can't get to them.

(U) Except for pi. Pi is the grand exception. It is the only transcendental number human beings have (there is also e, but pi and e are blood sisters so I'll consider them as one number here). I deliberately left pi out when I was constructing the set of all numbers up above. When numbers are constructed--integers, fractions, roots of equations, transcendentals--then properly at step 3 I should have put in not only roots of equations, but also physical constants. At the stage of complexity when human beings are inventing mathematical equations then they are also discovering physical constants that appear in equations--pi and e, the gravitational constant, Planck's constant, the speed of light, etc.

(U) I am not sure what happens with the other physical constants, but pi (which by definition is the circumference of a circle divided by

its diameter) has all sorts of mathematical properties. In particular, even though the definition of pi makes it sound as if we can only calculate pi by measuring things with rulers and string, pi is so snared up in mathematical formulas that we can compute it to all decimal places and, more significantly here, we can prove that it is transcendental.

(U) So I praise pi here because it allows me to glimpse the set of transcendental numbers, numbers which are otherwise unknowable to me, despite there being so overwhelmingly many of them.

(U) As a postscript I mention that in fact there are other known transcendentals, but the ones I know of were artificially constructed so I sneer at them. True numbers arise naturally. I could, however, be gracious and modify my statement above to "pi and a very few other, lesser, pipsqueak numbers are the only numbers that allow me to glimpse the vast, unknowable set of transcendental numbers."

****
//////////

6. (U//FOUO) PUZZLES: How Many Children? by [redacted]

(U) I hear children playing in the garden said Tony, a math graduate, are they all yours? No! Answered Professor White, the famous number theorist. My children are playing with the ones of three families in the neighborhood, even though our family is the most numerous one. The Browns have fewer children than us, the Greens even fewer, and the Blacks have the fewest. But, in total, how many children are they? asked Tony. Let us say, answered White, that in total they are fewer than eighteen, and the product of the four numbers equals the address of the house that you saw coming here.

(U) Tony pulled out his notepad and started to write. After a moment he asked: Do the Blacks have more than one child? As soon as Professor White answered, Tony gave the exact number of children in each family.

(U) How many children in each family?

(U//FOUO) Please send solutions to this puzzle to [redacted]
Please send new puzzle ideas to [redacted]
or [redacted]

(b)(3)-P.L. 86-36

****
//////////

7.(U) EDITORIAL CORNER

REMINDER: (U) Submissions for the next issue are due by 28 June, 1999.

PLEASE NOTE: (U) All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION-MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the editorial board.

(U//FOUO) _Tales of the KRYPT_ Editorial Board
Editor: [redacted]
Assistant Editor: [redacted]
Puzzle Editors: [redacted]

(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

[redacted]

\\\

~~SECRET//COMINT~~

(U) POC: [redacted] info
(U) *Last Modified: 10/30/2002 11:42:24*
(U) PE EXTERNAL PAGE

~~SECRET//COMINT-SPOKE//X1~~

(b)(3)-P.L. 86-36

****
* TALES OF THE KRYPT *
****
July - August 1999

//
****

++
//

(U) TABLE OF CONTENTS:

1. (U) Calendar of Events

2. (U//~~FOUO~~) Cryptanalysis Career Panel (CACP) Personnel Changes by [redacted] Executive, CACP

3. (U//~~FOUO~~) KRYPTOS Society Talk: Solution to a Major Portion of the CIA KRYPTOS Sculpture (Part I), by [redacted]

4. (~~C//SI~~) Technical Article: [redacted]

5. (U//~~FOUO~~) Preview of 1999 Cryptologic History Symposium, by [redacted] Center for Cryptologic History

6. (U) KRYPTOS Puzzle

   6a. (U//~~FOUO~~) New Puzzle: Number Sequences, by [redacted]

   6b. (U//~~FOUO~~) Solution to Previous Puzzle: How Many Children?, by [redacted]

7. (U) Editorial Corner

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

....
//

1. (U) CALENDAR OF EVENTS

Sep 14 (U//~~FOUO~~) KRYPTOS Society Talk, 1330 in Friedman Auditorium: the decipherment of a major portion of the the KRYPTOS sculpture at the CIA, by [redacted]

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

9/24/2010

(See article 3.)

(U) PLAN AHEAD

Oct 27-29 (U) Symposium on Cryptologic History, sponsored by the Center for Cryptologic History; Friedman Auditorium (See article 5.)

---

2. (U//~~FOUO~~) Cryptanalysis Career Panel (CACP) Personnel Changes by [redacted], Executive, CACP (b)(3)-P.L. 86-36

2a. (U) New CA Interns:

(U//~~FOUO~~) New hires - [redacted] and [redacted] started in July 1999. New on-board interns - [redacted] computer scientists, will be starting the CA intern program in September 1999.

2b. (U) CACP Personnel Changes

(U//FOUO) [redacted] current CA Panel Chair, has moved offices from Z09 to N2. (b)(3)-P.L. 86-36

(U) The CACP thanks the following:

(U//~~FOUO~~) [redacted] has rotated off the CA Panel and will be replaced by [redacted]. Welcome aboard, [redacted]

(U//~~FOUO~~) New Computer Program (CPEB) and Tech Paper Board (TPEB) members: Say "hello" to [redacted] and "goodbye" to [redacted] on the CPEB. [redacted] are replacing [redacted] on the TPEB. Welcome to [redacted] (b)(3)-P.L. 86-36

---

3. (U//~~FOUO~~) KRYPTOS Society News: Solution to a Major Portion of the CIA KRYPTOS Sculpture (Part I), by [redacted] will address this topic at the KRYPTOS Society meeting on Tuesday, 14 September, 1999 at 1330 in Friedman Auditorium.]

(U//~~FOUO~~) In the courtyard of the CIA's Headquarters complex is an unusual sculpture that doubles as a puzzle. More specifically, the puzzle is a set of enciphered messages. Earlier this year, a CIA employee claimed success in breaking the majority of these ciphers. In June, a private citizen in California did the same. NSA analysts also broke these same portions in 1992 after NSA was issued a challenge by the Director of Central Intelligence. With success on the outside though, now seems like a good time to tell this tale.

(U) INTRODUCTION (b)(3)-P.L. 86-36

(U) The following paper will take a technical look at the solution to

[redacted]

a major portion of the KRYPTOS sculpture located in the courtyard of the Central Intelligence Agency in Langley, Virginia. Before starting on the technical details, let's take a quick look at the history of the sculpture, as well as a few comments from the sculptor.

(U) In June 1988, a Fine Arts Commission project was announced by the CIA to acquire art work for the new CIA Headquarters building. When the selection process had been completed, the Director of Central Intelligence approved the proposal submitted by James Sanborn, a Washington (D.C.) area artist, to create a two-part sculpture at the west entrance to the new Headquarters building, and in the courtyard of the complex. In the fall of 1990 the work was unveiled at a dedication ceremony at the CIA.

(U) According to Mr. Sanborn, "the stonework at the entrance and in the courtyard served two functions. First, it creates a natural framework for the project as a whole and is part of a landscaping scheme designed to recall the natural stone outcropping that existed on the site before the Agency, and that will endure as do mountains. Second, the tilted strata tell a story like pages of a document. Inserted between these stone "pages" is a flat copper sheet through which letters and symbols have been cut. This code, which includes certain ancient ciphers, begins as International Morse and increases in complexity as you move through the piece at the entrance and into the courtyard. Its placement in a geologic context reinforces the text's "hiddenness" as if it were a fossil or an image frozen in time."

(U) This paper's purpose is to concentrate solely on the copper sheets located in the courtyard through which letters and question marks were cut out. It will look at the diagnosis, exploitation and eventual solution of the majority of the cipher contained in the sculpture.

(U) THE KRYPTOS SCULPTURE

(U) One half of the sculpture contains the following Vigenere Square, which uses mixed sequences based on the keyword KRYPTOS.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
A	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P
B	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T
C	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O
D	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S
E	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A
F	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B
G	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C
H	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D
I	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E
J	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F
K	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G
L	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H
M	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I
N	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L
O	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L
P	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M
Q	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N
R	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q
S	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U
T	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V

(b)(3)-P.L. 86-36

```
U  Q U V W X Z K R Y P T O S A B C D E F G H I J L M N Q U V W
V  U V W X Z K R Y P T O S A B C D E F G H I J L M N Q U V W X
W  V W X Z K R Y P T O S A B C D E F G H I J L M N Q U V W X Z
X  W X Z K R Y P T O S A B C D E F G H I J L M N Q U V W X Z K
Y  X Z K R Y P T O S A B C D E F G H I J L M N Q U V W X Z K R
Z  Z K R Y P T O S A B C D E F G H I J L M N Q U V W X Z K R Y
   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
```

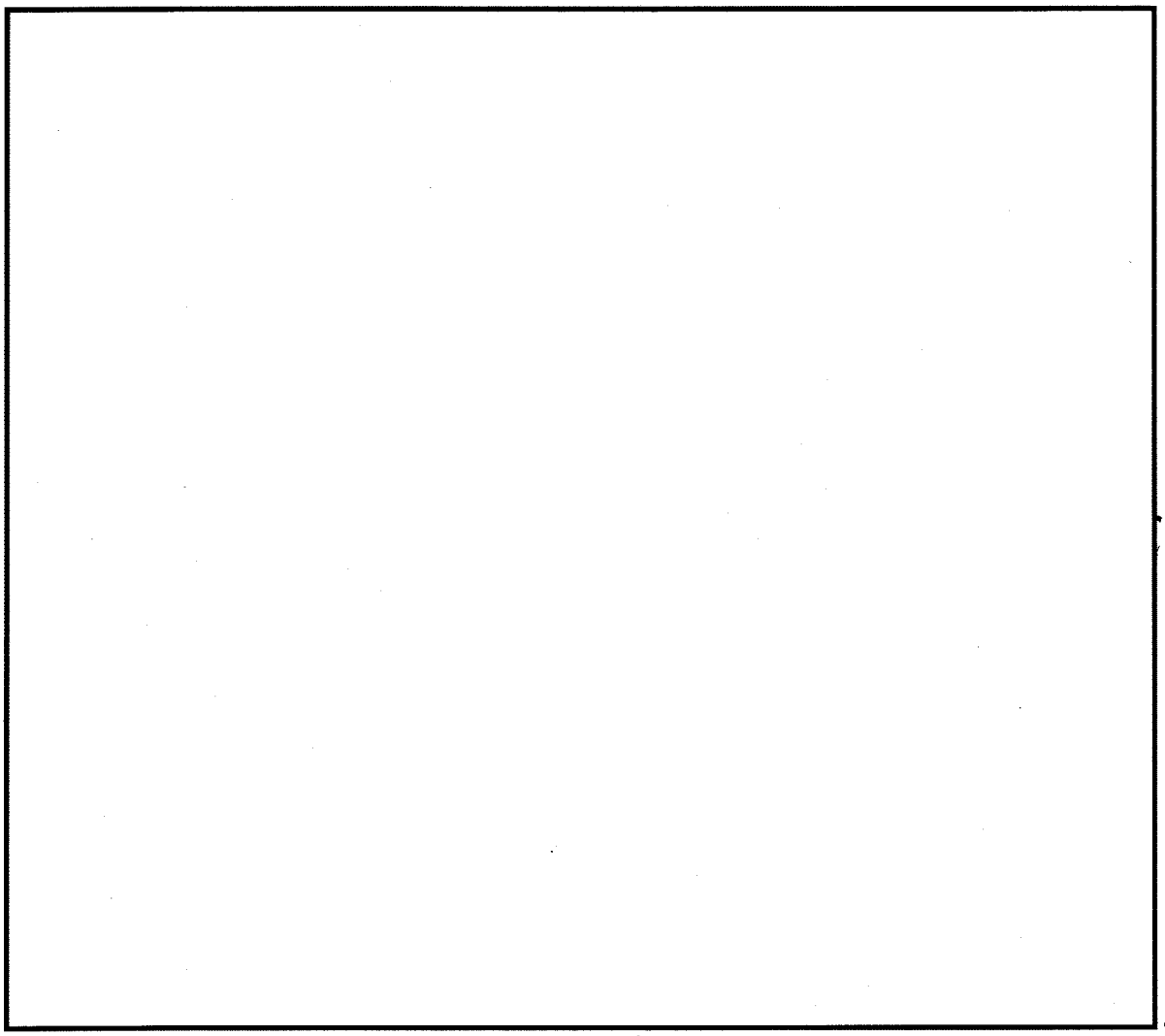
(U) Following is the other half of the main sculpture. Line numbers have been added for reference purposes only, and are not a part of the sculpture.

```
 1 E M U F P H Z L R F A X Y U S D J K Z L D K R N S H G N F I V J
 2 Y Q T Q U X Q B Q V Y U V L L T R E V J Y Q T M K Y R D M F D
 3 V F P J U D E E H Z W E T Z Y V G W H K K Q E T G F Q J N C E
 4 G G W H K K ? D Q M C P F Q Z D Q M M I A G P F X H Q R L G
 5 T I M V M Z J A N Q L V K Q E D A G D V F R P J U N G E U N A
 6 Q Z G Z L E C G Y U X U E E N J T B J L B Q C R T B J D F H J R R
 7 Y I Z E T K Z E M V D U F K S J H K F W E K U W Q L S Z F T I
 8 H H D D D U V H ? D W K B F U F P W N T D F I Y C U Q Z E R E
 9 E V L D K F E Z M O Q Q J L T T U G S Y Q P F E U N L A V I D X
10 F L G G T E Z ? F K Z B S F D Q V G O G I P U F X H H D R K F
11 F H Q N T G P U A E C N U V P D J M Q C L Q U M U N E D F Q
12 E L Z Z V R R G K F F V O E E X B D M V P N F Q X E Z L G R E
13 D N Q F M P N Z G L F L P M R J Q Y A L M G N U V P D X V K P
14 D Q U M E B E D M H D A F M J G Z N U P L G E W J L L A E T G
15 E N D Y A H R O H N L S R H E O C P T E O I B I D Y S H N A I A
16 C H T N R E Y U L D S L L S L L N O H S N O S M R W X M N E
17 T P R N G A T I H N R A R P E S L N N E L E B L P I I A C A E
18 W M T W N D I T E E N R A H C T E N E U D R E T N H A E O E
19 T F O L S E D T I W E N H A E I O Y T E Y Q H E E N C T A Y C R
20 E I F T B R S P A M H H E W E N A T A M A T E G Y E E R L B
21 T E E F O A S F I O T U E T U A E O T O A R M A E E R T N R T I
22 B S E D D N I A A H T T M S T E W P I E R O A G R I E W F E B
23 A E C T D D H I L C E I H S I T E G O E A O S D D R Y D L O R I T
24 R K L M L E H A G T D H A R D P N E O H M G F M F E U H E
25 E C D M R I P F E I M E H N L S S T T R T V D O H W ? O B K R
26 U O X O G H U L B S O L I F B B W F L R V Q Q P R N G K S S O
27 T W T Q S J Q S S E K Z Z W A T J K L U D I A W I N F B N Y P
28 V T T M Z F P K W G D K Z X T J C D I G K U H U A U E K C A R
```

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

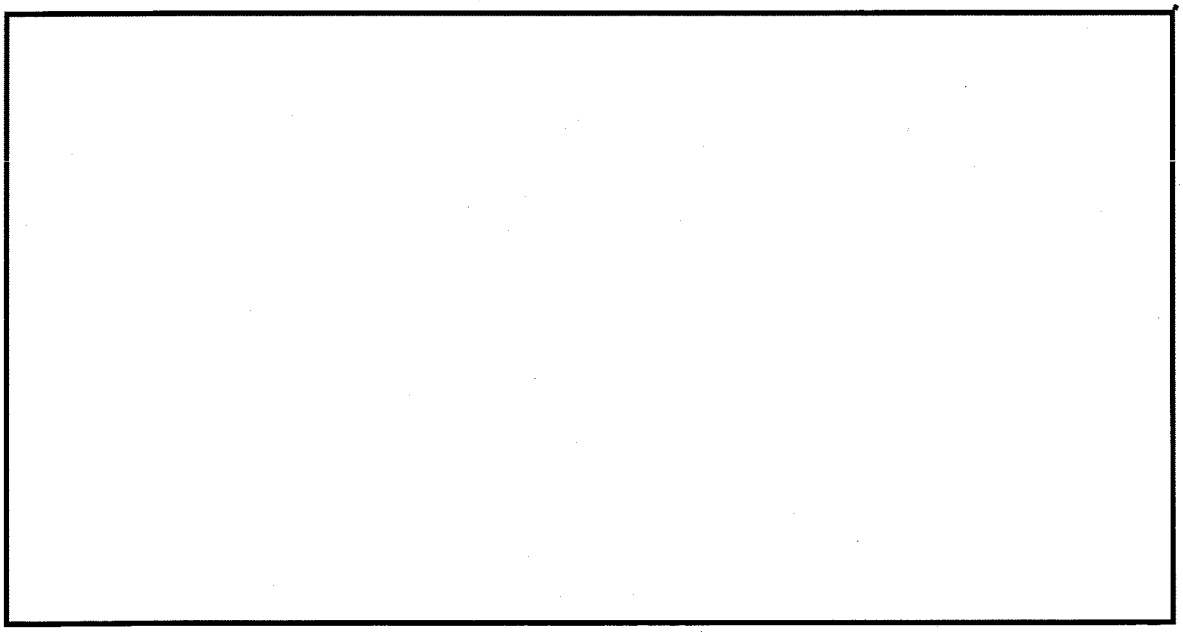
(U) DIAGNOSIS

(b)(3)-P.L. 86-36

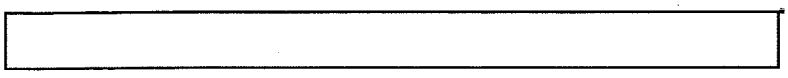


(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

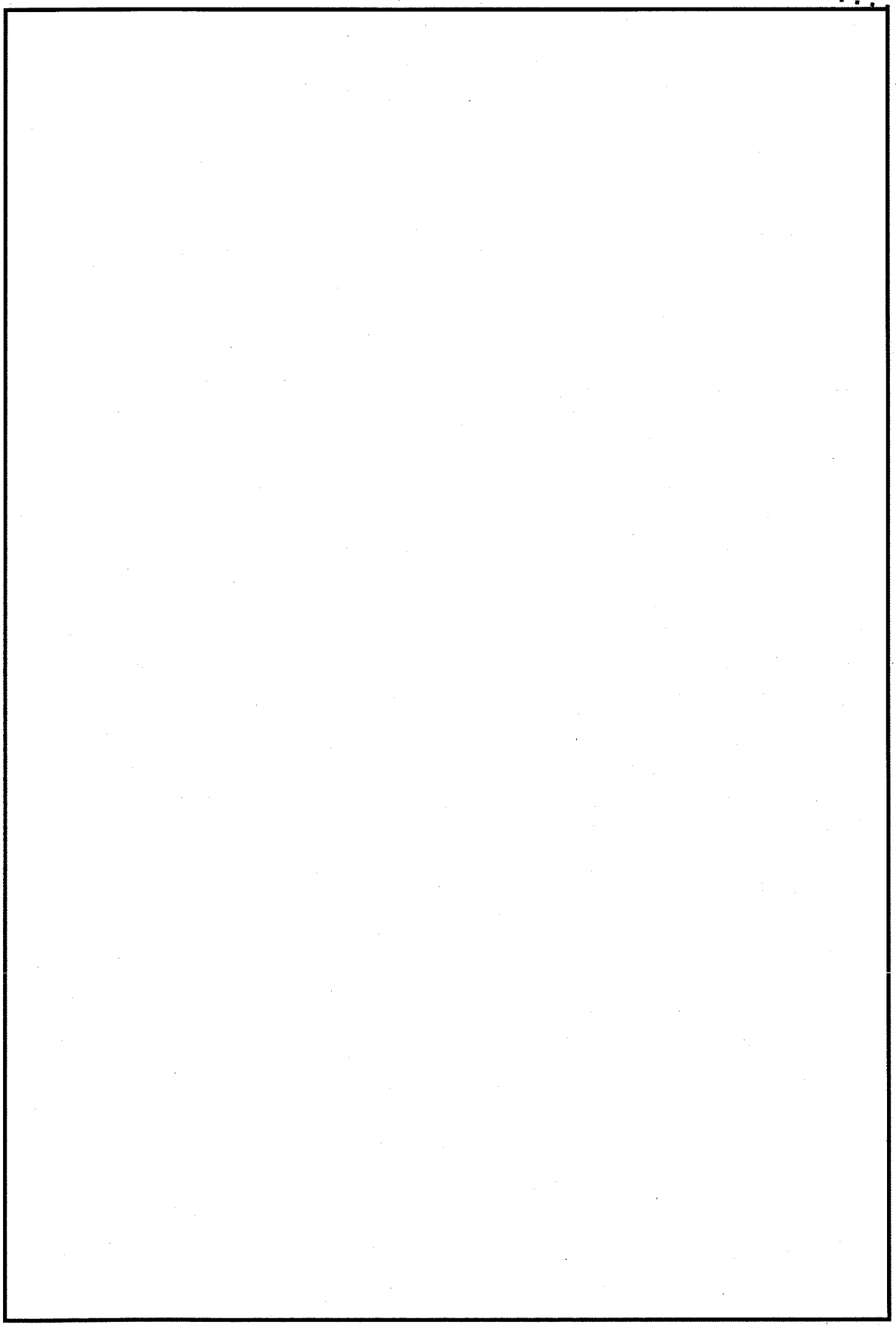
(U) THE FIRST BREAKTHROUGH



(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) Here is a more readable version, with punctuation added:

"IT WAS TOTALLY INVISIBLE. HOW'S THAT POSSIBLE? THEY USED THE EARTH'S MAGNETIC FIELD. THE INFORMATION WAS GATHERED AND TRANSMITTED UNDERGROUND TO AN UNKNOWN LOCATION. DOES LANGLEY KNOW ABOUT THIS? THEY SHOULD. IT'S BURIED OUT THERE SOMEWHERE. WHO KNOWS THE EXACT LOCATION? ONLY W.W. THIS WAS HIS LAST TRANSMISSION. THIRTY-EIGHT DEGREES, FIFTY-SEVEN MINUTES, SIX POINT FIVE SECONDS NORTH. SEVENTY-SEVEN MINUTES, FORTY-FOUR SECONDS WEST. I.D. BY ROWS."

(U) The reference to W.W. is presumed to be William Webster, former Director of the CIA. The coordinates given are a location within the CIA grounds, most likely the main complex or the courtyard area. The meaning of "I.D. BY ROWS" is not known at this time. The repeating key of ABSCISSA is defined by Webster's New World Dictionary as, "the horizontal Cartesian coordinate on a plane, measured from the y-axis along a line parallel with the x-axis to point P."

[redacted]

//

4. ~~(C//SI)~~ Technical Article: [redacted]

by [redacted] (b)(3)-P.L. 86-36

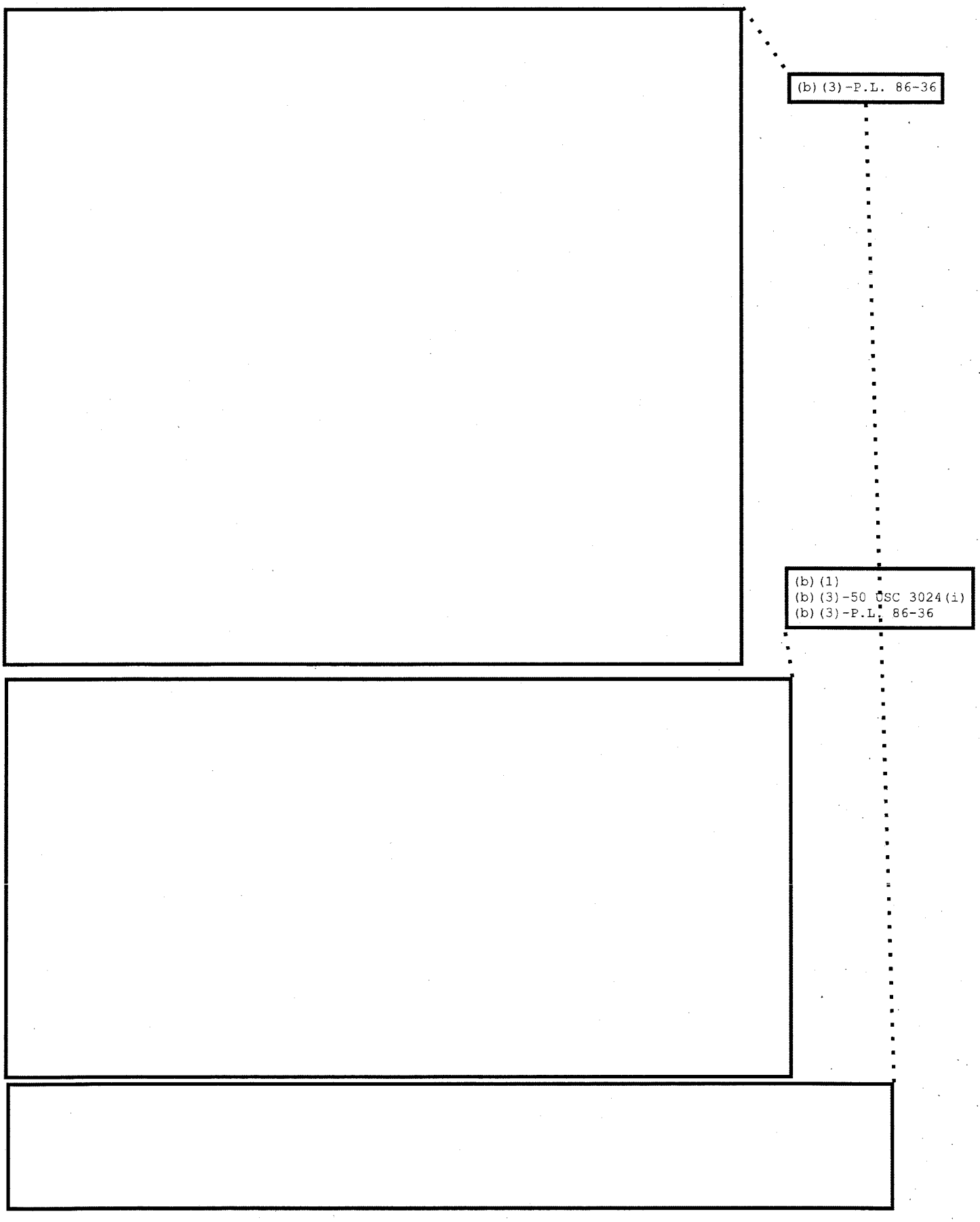
(b)(1)
(b)(3)-P.L. 86-36

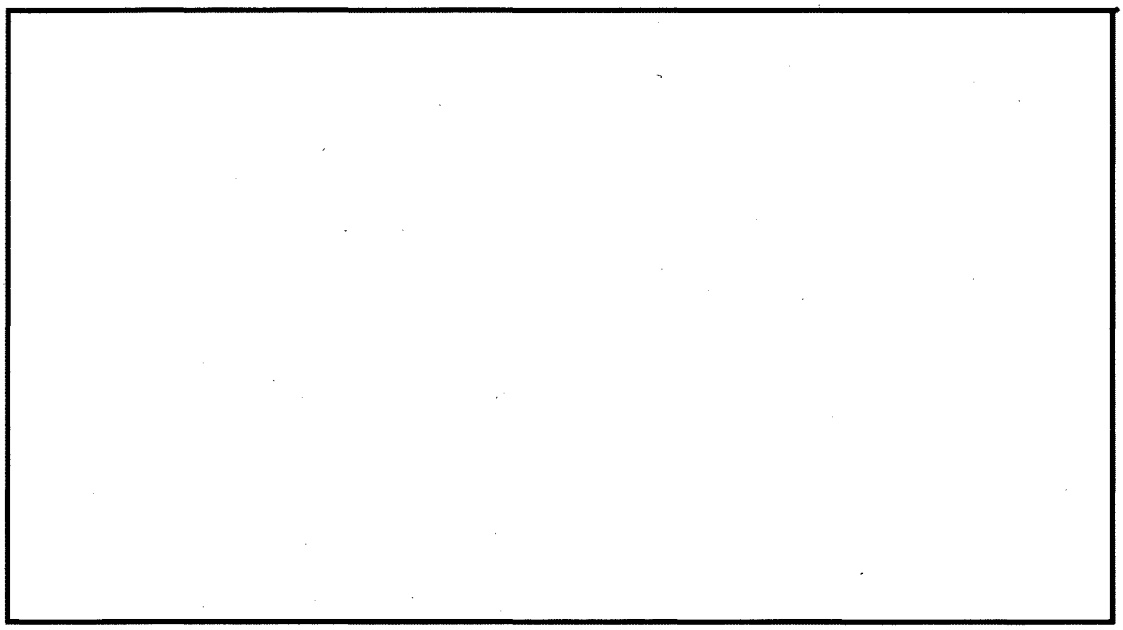
~~(C//SI)~~ The following article is based on a Z63 technical talk I gave on 21 June 1999. The talk was a general overview of [redacted] as well as the the work I completed as a CMP'er touring in Z631 from September 1998 through May 1999 to implement these concepts in a C programming environment.

[redacted]

(b)(3)-P.L. 86-36

[redacted]


(b)(3)-P.L. 86-36
(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

5. (U//~~FOUO~~) Preview of 1999 Cryptologic History Symposium, by Barry D. Carleen, Center for Cryptologic History

(U) The 1999 Symposium on Cryptologic History, sponsored by the Center for Cryptologic History, will be held in the Friedman Auditorium at NSA, Fort Meade, on 27, 28, and 29 October 1999. The Wednesday and Thursday sessions will run from approximately 8:30 a.m. to 4:00 p.m. The Friday session will run from 8:30 a.m. to 12:00 noon. All sessions will be unclassified.

(U) This year's symposium will take a retrospective look at a century of signals intelligence and information systems security. It will also provide fresh insights into the uses of cryptology in World War II and in counterespionage activities, such as VENONA and ISCOT. Other presentations will discuss selected topics in cryptology and the Cold War. In addition, the symposium will feature a panel discussion on the declassification process currently underway in the Intelligence Community.

(U) We will keep you informed about the progress of planning for the symposium, and we will send out a calendar of speakers about 1 October.

6. (U) KRYPTOS Puzzle

6a. (U//~~FOUO~~) New Puzzle: Number Sequences, by [redacted]

(U) The 12 sequences below all have a logical pattern. For each sequence, find the number that goes in the blank and give a brief description of the method of generation. Occam's Razor applies. The winners will be chosen based on the number of correct answers.

(U) A. 1 1 2 3 5 8 13 21 ____

(b)(3)-P.L. 86-36

[redacted]

(U) B. 1 1 2 3 5 11 26 81 ____

(U) C. 1 2 4 7 9 12 18 24 32 ____

(U) D. 1 2 4 8 16 23 28 38 49 62 ____

(U) E. 1 2 4 7 8 11 13 14 16 19 21 22 25 26 ____

(U) F. 1 4 8 13 19 23 30 35 43 50 54 ____

(U) G. 2 3 6 2 3 6 6 2 5 2 4 1 4 7 ____

(U) H. 1 5 9 13 21 23 29 33 45 53 61 ____

(U) I. 36 67 93 142 483 889 1790 2800 ____

(U) J. 21 36 55 60 67 68 92 93 ____

(U) K. 1 3 11 19 37 55 ____

(U) L. 101 118 215 531 705 ____

Editor's Comments

I. This one's pretty far out.
J. You'll sing with joy when you get this.
K. This is elementary.
L. You're done. You deserve a break.

(U//~~FOUO~~) Please send solutions to this puzzle to [redacted] at [redacted] Please send new puzzle ideas to [redacted] or [redacted]

(b)(3)-P.L. 86-36

- - -

6b. (U//~~FOUO~~) Solution to Previous Puzzle: How Many Children?, by [redacted]

(U) I hear children playing in the garden said Tony, a math graduate, are they all yours? No! Answered Professor White, the famous number theorist. My children are playing with the ones of three families in the neighborhood, even though our family is the most numerous one. The Browns have fewer children than us, the Greens even fewer, and the Blacks have the fewest. But, in total, how many children are they? asked Tony. Let us say, answered White, that in total they are fewer than eighteen, and the product of the four numbers equals the address of the house that you saw coming here.

(U) Tony pulled out his notepad and started to write. After a moment he asked: Do the Blacks have more than one child? As soon as Professor White answered, Tony gave the exact number of children in each family.

(U) How many children in each family?

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Correct solutions were submitted by: [redacted]

[redacted]

[redacted]

[redacted] Here is the solution submitted by [redacted] (IDA/CCS):

(b)(3)-P.L. 86-36

(U) Given:

White Brown Green Black 0
White + Brown + Green + Black < 18
White * Brown * Green * Black = Address

(U) Here are the possible choices for (Bl,Gr,Br,Wh) and their product:

1,2,3,4-11	24,30,36,42,48,54,60,66
1,2,4,5-10	40,48,56,64,72,80
1,2,5,6-9	60,70,80,90
1,2,6,7-8	84,96
1,3,4,5-9	60,72,84,96,108
1,3,5,6-8	90,105,120
1,3,6,7	126
1,4,5,6-7	120,140
2,3,4,5-8	120,144,168,192
2,3,5,6-7	180,210
2,4,5,6	240

(U) We assume that Tony could not determine the number of children from the address, because there was not a unique answer. This limits the choices to the following:

48 = 1*2*3*8 = 1*2*4*6
60 = 1*2*3*10 = 1*2*5*6 = 1*3*4*5
72 = 1*2*4*9 = 1*3*4*6
80 = 1*2*4*10 = 1*2*5*8
84 = 1*2*6*7 = 1*3*4*7
90 = 1*2*5*9 = 1*3*5*6
96 = 1*2*6*8 = 1*3*4*8
120 = 1*3*5*8 = 1*4*5*6 = 2*3*4*5

(U) When Tony was told whether the Blacks had more than one child, he was able to answer correctly. Assuming that he didn't just guess but could deduce the answer, the address must be 120 and the Professor must have said that the Blacks have two children.

(U) Thus there are 14 children in the garden:
5 Whites, 4 Browns, 3 Greens and 2 Blacks.

"""""""

Assistant Editor:
Puzzle Editors:

[redacted]

(b)(3)-P.L. 86-36

[redacted]

\\\

~~SECRET//COMINT//NOFORN//X1~~

(C) POC: [redacted] info
(U) *Last Modified: 10/30/2002 11:42:25*
(U) PE EXTERNAL PAGE

~~SECRET//COMINT//NOFORN//X1~~

****
* TALES OF THE KRYPT *
****
September - October 1999

//
****

(b)(3)-P.L. 86-36

++
//

(U//~~FOUO~~) TABLE OF CONTENTS:

1. (U//~~FOUO~~) Perspective: "Memories of My Three Years as CACP Exec" by [redacted]

2. (U) Calendar of Events

3. (U//~~FOUO~~) Cryptanalysis Career Panel (CACP) News:

3a. (U//~~FOUO~~) New CA Interns

3b. (U//~~FOUO~~) CACP Personnel Changes

3c. (U) Congratulations!

3d. (U//~~FOUO~~) FY00 Hiring

4. (U//~~FOUO~~) KRYPTOS Society News: Annual KRYPTOS Society Luncheon

5. (U) Technical Articles

5a. (U//~~FOUO~~) "Some New Lattice Quantization Algorithms For Videoconferencing" by [redacted]

5b. (U//~~FOUO~~) "Solution to a Major Portion of the CIA KRYPTOS Sculpture" (Part II), by [redacted]

6. (U//~~FOUO~~) Community News: "Congratulations Class of 1999 Cryptologic Mathematician Program (CMP)" by: [redacted]

7. (U//~~FOUO~~) KRYPTOS Puzzle:

7a. (U//~~FOUO~~) New Puzzle: "Disemvoweled" by [redacted]

7b. (U//~~FOUO~~) Solution to Previous Puzzle: "Number Sequences" by [redacted]

8. (U) Editorial Corner

(b)(3)-P.L. 86-36

//

1. (U//~~FOUO~~) PERSPECTIVE: "Memories of My Three Years as CACP Exec" by [redacted]

(U//~~FOUO~~) Each issue of this newsletter features the perspective of a Senior on a CA topic of his/her choice. This issue we are pleased to feature the thoughts of [redacted] previous Cryptanalysis Career Panel Executive.

(U//~~FOUO~~) I was a little surprised when I was asked to write a perspective on my term as Executive of the Cryptanalysis Career Panel for _Tales of the KRYPT_, since I didn't feel that I had any particular insight into the field or the future of Crypt-analysis because of my position. Nevertheless, it was a very

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

enlightening experience, and I would definitely encourage every cryppie to spend some time outside of Z in a similar position to see what the Agency is all about.

(U//FOUO) In some ways, I learned more about cryptanalysis at NSA during my three years in this non-technical job than I did working in the trenches. I got to meet a lot of people doing CA in different parts of the Agency that I never would have known about otherwise. I also got a good picture of NSA from this vantage point. From where I sat in DS, I saw the Agency as a business--the running of a large corporation--and not just 'SIGINT as far as the eye can see'. We were the first to hear about new initiatives like doing away with professionalization, P3, and the new promotion process. Another benefit of this job was getting to meet and work closely with some very senior people at NSA. Because of the office I represented, I had some power and people listened to what I had to say (or at least pretended to!).

(U//FOUO) At first, being surrounded by non-techies took some getting used to. I felt like a fish out of water in the "touchy-feely" Human Resources world. I brought a very analytical approach to all my human resources activities, and I believe many of my HR counterparts were amused (but impressed) at my scientific/ logical approach to soft subjects.

(U//FOUO) On the down side, I missed the great technological support we had in Z Group. The system admins supporting the career panel office in OPS 2B were out at FANX and we never knew a name or phone number to call--you had to submit a "ticket" through Netscape, which was impossible to do if your computer was down!. (Which was usually why you needed them...) Calling up a Frame document took 10 minutes and printing it out took even longer. Still, in spite of this we managed to get our work done (often by getting help from Z Group which, for instance, loaned us sun terminals when we couldn't get any from our own organization).

(U//FOUO) Although I was in the same position for three years, there was quite a bit of diversity:

(U) Diagnosis

(U//FOUO) Occasionally an intern or cross-trainee would come in disheartened and discouraged, perhaps wanting to quit the program, and it would be up to the Exec(s) to figure out what was at the root of the problem and how to solve it.

(U//FOUO) Attack Development

(U//FOUO) We were quite frequently given a problem and would have to decide how to tackle it, such as "Professionalization is going away. How are we going to do life-long career development?" or "The CA career field is having an identity crisis. What are we going to do about it?"

(U) Exploitation

(U//FOUO) Exploitation of the CA workforce was one of my favorite pastimes. When people saw my sid in their mailbox they quickly learned to delete the email sight unseen, knowing that I was probably tapping them for some task or other. But the truth is that the CACP couldn't do its job without the help of all the dedicated volunteers throughout the community, whether serving on an official panel for certification or tech track, taking a trainee into their office for six months, being part of an ad hoc working group for some CA issue, or a myriad other things. To all of you I extend my deepest thanks. The CA workforce was very responsive to my requests for help, and usually readily stepped forward to volunteer its time and efforts (except in the case of replacing the Execs when it was our time to move on...) Some were called on more than others, and had barely gotten off one board/committee only to be put on another! (You know who you are, and we are so grateful for you!)

(U) Research

(U//FOUO) There was plenty of work done in this area.

(b)(3)-P.L. 86-36

We were forever getting bombarded with requests for obscure information like "How many CA intern graduates since the beginning of time have...." and "How many females certified in CA are also Senior Members or above in the Tech Track?" Sometimes an issue would arise at a Career Panel meeting, such as "How well do CQB scores predict future success in the field?" and I was off and running collecting data, doing analysis and drawing conclusions.

(U) Despite keeping up in these diversity areas, time and technology have marched on. Trying to get back into a highly technology-based job after a three-year hiatus is tough. But in spite of that, I would do it again.

(U//FOUO) So to answer the question I was asked to write about, the major things affecting the cryptanalytic field that happened during my tenure in office were A) a broader view of what constitutes cryptanalysis, B) a permanent and expanded technical track program, and C) renewed hiring into the CA career field. But those are not the things I will remember most vividly from my experience as a cultural exchange student from DO in DS.

"""""""

Panel.

(U//FOUO) [redacted] is the CACP's new Administrative Assistant.

3d. (U//FOUO) Newly Certified Cryptanalysts

(U//FOUO) Congratulations to the following newly certified cryptanalysts!

[redacted] (b)(3)-P.L. 86-36

3e. (U//FOUO) FY00 Hiring

(U//FOUO) The CACP will be able to hire [redacted] interns in FY00.

"""""""

by [redacted] (b)(3)-P.L. 86-36

1. (U) Introduction

(U//~~FOUO~~) Motion compensation is a technique for compressing video data. Since there is very little change between 2 frames of data we would like to code the changes rather than the entire picture every time. This is accomplished by predicting where the objects in the picture will move and describing this motion using motion vectors. Since motion is not always uniform, we will quickly have the problem of error propagation.

(U//~~FOUO~~) A patent by Baker, et. al. describes an innovative method for correcting the error by encoding it using a technique called lattice quantization. The errors are taken 8 pixels at a time to form an 8-long vector. By exploiting various symmetries, Baker can reconstruct the 2400 most likely vectors (excepting the all 0's vector) by storing only 920 of them. This article will present an improved technique in which all 2400 vectors can be recovered by storing only the 16 codewords of the 8-long extended Hamming code (defined below), an enormous reduction of storage requirements. This work is covered by three patent applications recently submitted by NSA to the U.S. Patent office.

2. (U) Lattices and Lattice Quantization

(U//~~FOUO~~) We start with some definitions. A quantizer is a device which converts numerical data into a finite number of possible outputs. A scalar quantizer rounds a real number to the nearest allowed output value. A vector quantizer takes a point in Rn (i.e. a point having n coordinates) to the nearest point taken from a set of points that has been precomputed so that there are more allowed points in areas of higher probability and less in areas of lower probability. Any quantizer produces round-off error. A vector quantizer produces less error on the average, but it is much more complicated than a scalar quantizer.

(U//~~FOUO~~) An alternative form of vector quantization is called lattice quantization. A lattice can be thought of as an evenly spaced grid in space. Put more precisely, given n linearly independent vectors x1,...,xn in Rn, the lattice generated by x1,...,xn is the set of points (c1 x1+...+cn xn) where c1,...,cn are all integers. We can use a lattice for quantization by rounding our input point to the nearest lattice point. This requires no precomputation, but now there are infinitely many possible outputs. Because of this fact, lattice quantization is only appropriate for data whose probability distribution is heavily concentrated around a single point. In our case, we are dealing with error vectors, so our data is heavily concentrated around the origin of Rn.

3. (U) Baker's Method and Our Improvement

(U//~~FOUO~~) For his lattice quantizer, Baker used a special lattice known as E8. The points of E8 have 8 coordinates and they are of the form (x1,...,x8) or (x1+.5,...,x8+.5) where in either case x1,...,x8 are all integers, and x1+...+x8 is an even number. E8 is currently the best known quantizer in 8 dimensions in the sense that it has a smaller roundoff error than any other known lattice in R8. E8 also has the property that for any point (y1,...,y8) in E8, the sum of the squares of the coordinates is an even integer. If y1y1+...+y8y8=2i, we say that the point (y1,...,y8) is in shell i.

(U//~~FOUO~~) For Baker's error data, 90% of the points round to the origin and 8-9% round to points in shells 1 and 2. The interesting part of the patent describes the coding of the points in the first 2 shells. There are 240 points in shell 1 and 2160 points in shell 2 totalling 2400 points. If a point (y1,...,y8) is in shell i of E8 (i=1, 2), then (-y1,...,-y8) is also in E8 and also in shell i. So we only have to remember 1200 points, since the remaining points are just their negatives. By exploiting additional symmetry, we can reduce this number further so that only 920 points need to be stored.

(U//~~FOUO~~) Our improvement uses a different version of the

(b)(3)-P.L. 86-36

[redacted]

E8 lattice involving the 8-long extended Hamming code, a well known error correcting code. We will avoid a long discussion here on error correcting codes, but this code can be thought of as a set of 16 8-bit words with the property that any 2 of them differ in at least 4 places. We say that a point (y1,...,y8) is in this alternate E8 lattice if multiplying each coordinate by the square root of 2 and taking the result modulo 2 produces a word in the extended Hamming code. This implies that the yi are in the form of an integer divided by the square root of 2. The new E8 lattice can be thought of a "rotated" version of the one used by Baker.

(U//~~FOUO~~) In our new version we only need to store the 16 words of the extended Hamming code instead of the 920 points needed by Baker. Ignoring the factor of one divided by the square root of 2, all of the shell 1 and 2 points consist of codewords with the 1's possibly replaced by -1's and the 0's possibly replaced by 2's or -2's. We can send these points with the same number of bits needed by Baker.

4. (U) A Leech Lattice Quantizer

(U//~~FOUO~~) We have also designed a quantizer using a 24-dimensional lattice known as the Leech lattice. There are a number of advantages to this. First of all, a number of very fast algorithms exist for finding the closest point of the Leech lattice to a given point with 24 coordinates. Secondly, the Leech lattice has a smaller average error than any known lattice in equal or smaller dimension. We can also send 3 times the information as with the E8 lattice. Finally, the Leech lattice has played an important role in mathematics, especially in the classification of finite simple groups. For this reason, it has been extensively studied.

(U//~~FOUO~~) For more information and the mathematical details, see my paper "An Introduction to the Theory of Lattices" which is available on request.

5b. (U//~~FOUO~~) "Solution to a Major Portion of the CIA KRYPTOS Sculpture (PART II), by [redacted]

(b)(3)-P.L. 86-36

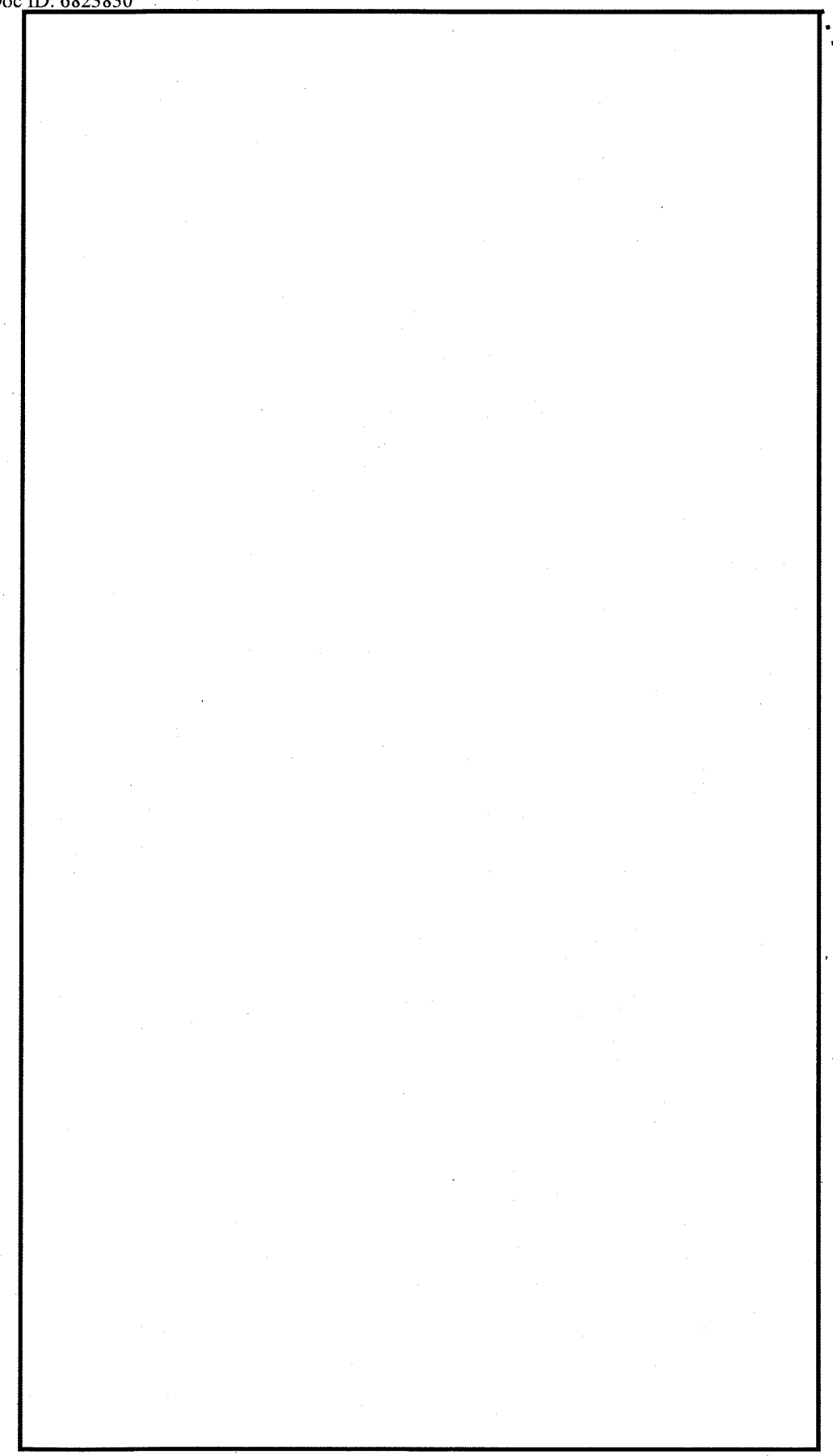
I.(U) The Second Breakthrough

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

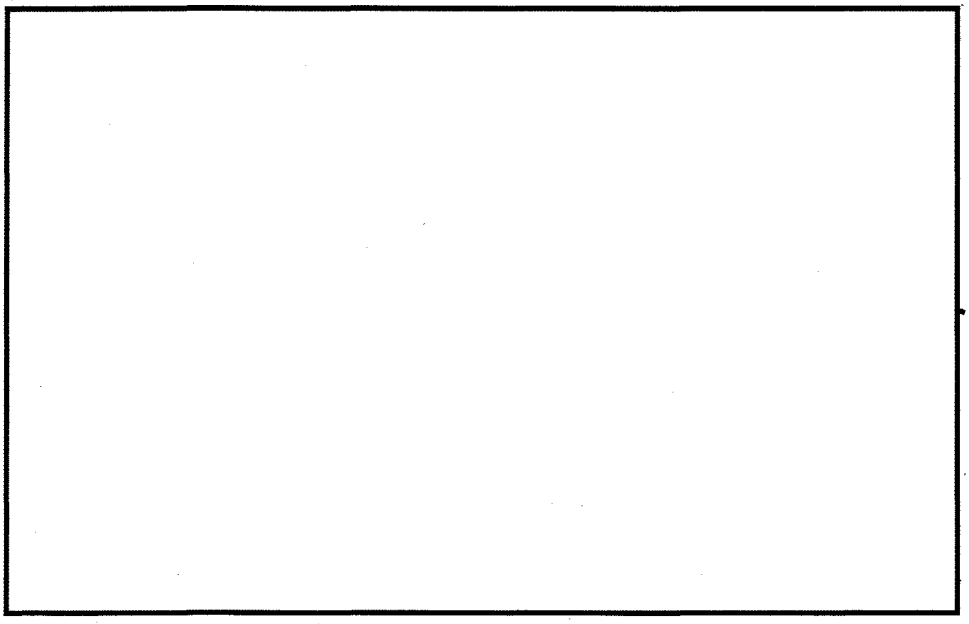
(b)(3)-P.L. 86-36

[redacted]



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

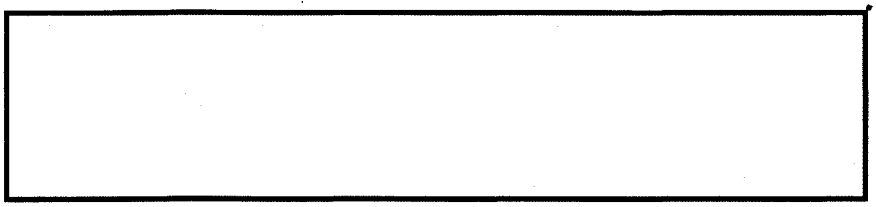
(b)(3)-P.L. 86-36



(b)(3)-P.L. 86-36

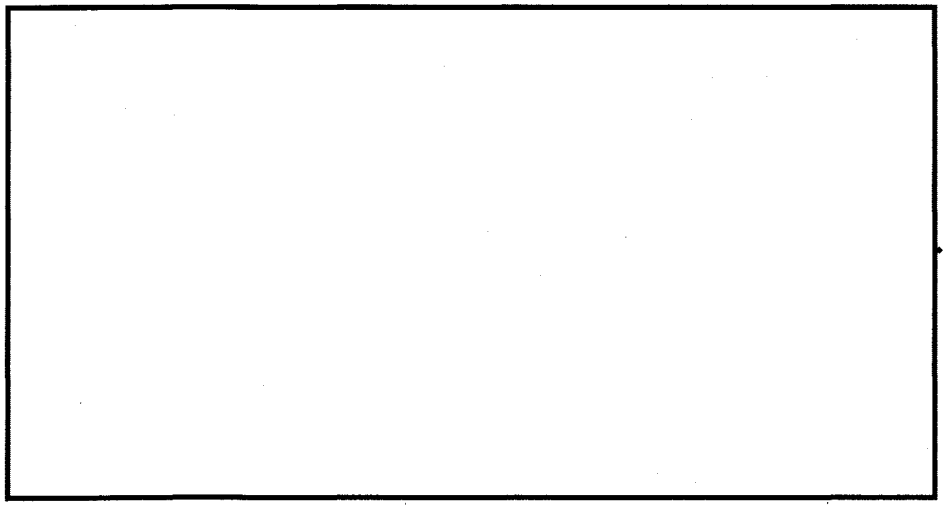
(U) Although this may or may not be the way the system was originally set up by Sanborn, it is likely to be very close to the truth. The entire text of section 3 follows, with appropriate punctuation:

"SLOWLY DESPARATELY SLOWLY THE REMAINS OF PASSAGE DEBRIS THAT ENCUMBERED THE LOWER PART OF THE DOORWAY WAS REMOVED. WITH TREMBLING HANDS I MADE A TINY BREACH IN THE UPPER LEFTHAND CORNER, AND THEN, WIDENING THE HOLE A LITTLE, I INSERTED THE CANDLE AND PEERED IN. THE HOT AIR ESCAPING FROM THE CHAMBER CAUSED THE FLAME TO FLICKER, BUT PRESENTLY, DETAILS OF THE ROOM WITHIN EMERGED FROM THE MIST X CAN YOU SEE ANYTHING Q"



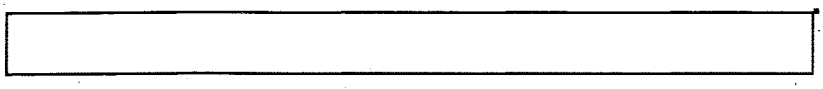
(U) If you have ever read about King Tut, the passage may have sounded familiar to you. It is a paraphrasing from the book "The Tomb of Tut-ankh-amen" written by Howard Carter.

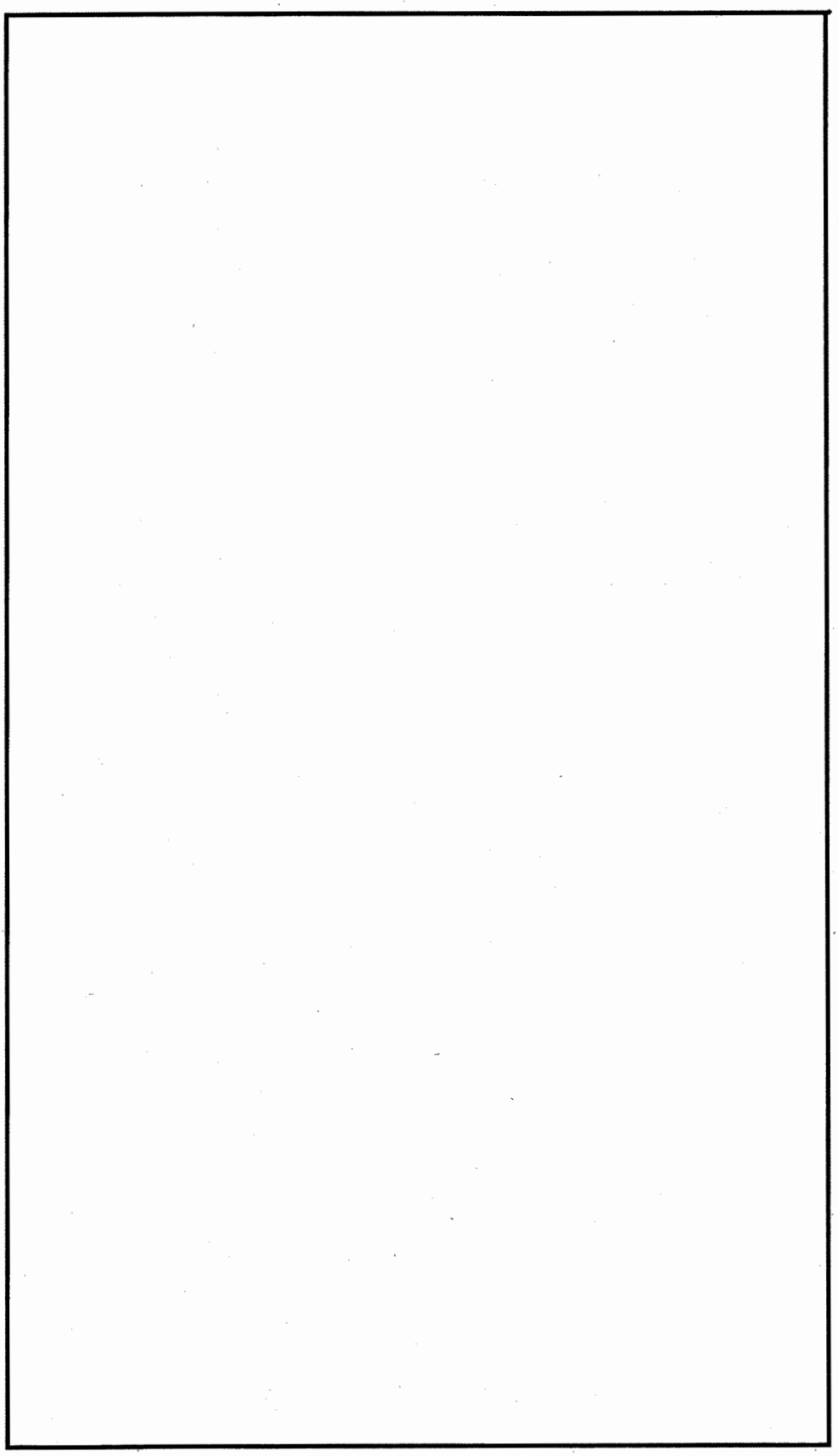
II.(U) The Third Breakthrough



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

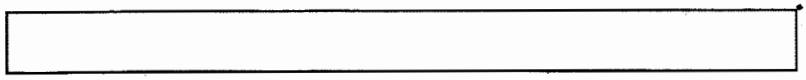




(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(U//~~FOUO~~ Respaced and punctuated, it reads:



"BETWEEN SUBTLE SHADING AND THE ABSENCE OF LIGHT LIES THE NUANCE OF ILLUSION"

[redacted]

III.(U) The Fourth Breakthrough?

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

IV.(U) Recap

[redacted]

The plain text reads:

"BETWEEN SUBTLE SHADING AND THE ABSENCE OF LIGHT LIES THE NUANCE OF ILLUSION"

[redacted]

"IT WAS TOTALLY INVISIBLE. HOW'S THAT POSSIBLE? THEY USED THE EARTH'S MAGNETIC FIELD. THE INFORMATION WAS GATHERED AND TRANSMITTED UNDERGROUND TO AN UNKNOWN LOCATION. DOES LANGLEY KNOW ABOUT THIS? THEY SHOULD. IT'S BURIED OUT THERE SOMEWHERE. WHO KNOWS THE EXACT LOCATION? ONLY W.W. THIS WAS HIS LAST TRANSMISSION. THIRTY-EIGHT DEGREES, FIFTY-SEVEN MINUTES, SIX POINT FIVE SECONDS NORTH. SEVENTY-SEVEN MINUTES, FORTY-FOUR SECONDS WEST. I.D. BY ROWS."

[redacted]

The plain text reads:

"SLOWLY DESPARATELY SLOWLY THE REMAINS OF PASSAGE DEBRIS THAT ENCUMBERED THE LOWER PART OF THE DOORWAY WAS REMOVED. WITH TREMBLING HANDS I MADE A TINY BREACH IN THE UPPER LEFTHAND CORNER, AND THEN,

(b)(3)-P.L. 86-36

[redacted]

WIDENING THE HOLE A LITTLE, I INSERTED THE CANDLE AND PEERED IN. THE HOT AIR ESCAPING FROM THE CHAMBER CAUSED THE FLAME TO FLICKER, BUT PRESENTLY, DETAILS OF THE ROOM WITHIN EMERGED FROM THE MIST. CAN YOU SEE ANYTHING?"

[redacted]

(b)(3)-P.L. 86-36

6. (U//~~FOUO~~) Community News: "Congratulations Class of 1999 Cryptologic Mathematician Program (CMP)" by [redacted]

(U//~~FOUO~~) On 1 October 1999 in the Friedman Auditorium, the 34th class of the Cryptologic Mathematician Program (CMP) graduated. The Master of Ceremonies was [redacted] Executive, CMP. The opening remarks were made by [redacted] Chief, Techniques and Research. Mr. James R. Taylor, Deputy Director for Operations, gave the keynote address. Various members of the Agency mathematics community attended the event, along with other Agency personnel, family members, friends and Agency retirees.

(U) During their three year program, class members attended many training classes, conferences and went on a variety of class trips.

[redacted]

The following is a list of the graduates and their first assignment after graduation:

[redacted]

* Barbershop
** CryptoScience Fellowship Program
*** K Group Math Office

7. (U) KRYPTOS PUZZLE

7a. (U//~~FOUO~~) New Puzzle: "Disemvoweled," by [redacted]

(U) Each of the following is a group of related words. Each group has had its vowels removed (ouch!). For purposes of this puzzle, Y is always a consonant. The number in brackets indicates the number of words in the group. For each group, fill in the missing vowels, and identify the common feature.

Example:

[6] P D L B G L C L L B X R T R R R C H H H

would be six breeds of dogs:

Poodle Beagle Collie Boxer Terrier Chihuahua

(b)(3)-P.L. 86-36

[redacted]

(U//FOUO) There are a baker's dozen here, so enjoy! Feel free to submit partial solutions. (Thanks to [redacted] for suggesting this type of puzzle.)

(U) [6] B S L R G N D L L C R N D R C M N M G

[4] C N N M L R N C S R B C S P D

[6] K R C H N R S S L S N P L N D

[5] R L S M T S N G L S P D R S X P S

[6] R S D S Y R S P T N B G N D H L

[6] P L J V B S C C C B L D

[6] B V L T B C L L F L T P N

[6] W H T W H T C H P T P T N N R Y

[5] M R M G R T T D L M S S N R N S T

[6] B L S K T Y D D M T H B T L N T

[5] L S T N M N N W R Z N T T N C B N T Y

[6] M R M N N Q N S H R D Y W L F P N

[6] T M T P F F F F N R D R R C K M D S M G

(U//FOUO) Please send solutions to this puzzle to [redacted] at [redacted] Please send new puzzle ideas to [redacted] or [redacted]

(b)(3)-P.L. 86-36

7b. (U//FOUO) Solution to Previous Puzzle: "Number Sequences", by [redacted]

(U//FOUO) The 12 sequences below all have a logical pattern. For each sequence, find the number that goes in the blank and give a brief description of the method of generation.

A. 1 1 2 3 5 8 13 21 _34_
Fibonacci sequence, x_i = x_{i-1} + x_{i-2}

B. 1 1 2 3 5 11 26 81 _367_
x_i = x_{i-1} + (x_{i-2} * x_{i-3})

C. 1 2 4 7 9 12 18 24 32 _38_
x_i = x_{i-1} + the number of factors of x_{i-1}

D. 1 2 4 8 16 23 28 38 49 62 _70_
x_i = x_{i-1} + sum of digits of x_{i-1}

E. 1 2 4 7 8 11 13 14 16 19 21 22 25 26 _28_
Numbers whose density of 1's in binary is odd. (poppar(x) = 1)

F. 1 4 8 13 19 23 30 35 43 50 54 _61_
x_i = x_{i-1} + number of distinct letters used to spell x_{i-1}

G. 2 3 6 2 3 6 6 2 5 2 4 1 4 7 _5_
Number of letters in each word of the US Constitution.
(We the people of the United States ... union)

H. 1 5 9 13 21 23 29 33 45 53 61 _63_
Years in the 20th century in which a new U.S. president took office

I. 36 67 93 142 483 889 1790 2800 _3670_
Millions of miles from planets to sun (closest to furthest).
This question had a wide range of possible answers depending on the source, but any reasonable value was accepted

J. 21 36 55 60 67 68 92 93 _125_

(b)(3)-P.L. 86-36

[redacted]

Beethoven symphony opus numbers

K. 1 3 11 19 37 55 _87_
Atomic numbers of elements reading down the 1st column of the periodic table

L. 101 118 215 531 705 _906_
Federal holidays in 1999 (given month/day)

(U//~~FOUO~~) A complete solution was submitted by [redacted] Honorable mention goes to [redacted]

(b)(3)-P.L. 86-36

8.(U) EDITORIAL CORNER

REMINDER: (U) Submissions for the next issue are due by 21 October, 1999.

PLEASE NOTE: (U//~~FOUO~~) All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION-MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the editorial board.

(U//~~FOUO~~) _Tales of the KRYPT_ Editorial Board

Editor: [redacted]
Assistant Editor: [redacted]
Puzzle Editors: [redacted]

(b)(3)-P.L. 86-36

~~SECRET//COMINT//X1~~

Derived from: NSA Class. Guide 342-98
3 August 1998
Declassify on: X1

DERIVED FROM: NSA/CSSM 123-2, DATED 3 SEP 1991
DECLASSIFY ON: SOURCE MARKED "OADR" DATE OF SOURCE: 3 SEP 1991

~~SECRET//COMINT~~

(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

(U) POC: [redacted] info
(U) Last Modified: 10/30/2002 11:42:24
(U)PE EXTERNAL PAGE

[redacted]

****
* TALES OF THE KRYPT *
****
November - December 1999

//
****

++
//

(U) TABLE OF CONTENTS:

1. (U//[redacted]) Perspective: Introductory Remarks at the Annual KRYPTOS Society Luncheon by [redacted], President of the KRYPTOS Society

2. (U) Calendar of Events

3. (U) Cryptanalysis Career Panel News: Sixth Annual Breakfast Affair for Newly Certified Cryptanalysts (BANCC)

4. (U) KRYPTOS Society News

4a. (U) KRYPTOS Society Election Results

4b. (U//[redacted]) CSE KRYPTOS Election Results by [redacted], Secretary, CSE Chapter of the KRYPTOS Society For [redacted], 1999 President, CSE Chapter of the KRYPTOS Society

4c. (U//[redacted]) KRYPTOS Society Peter Tenks Award -- for [redacted] ZB (Presentation Address by [redacted], President of the KRYPTOS Society)

4d. (U//[redacted]) KRYPTOS Society Norman Roberts Award -- for [redacted] (Presentation Address by [redacted], President-Elect of the KRYPTOS Society)

4e. (U//[redacted]) KRYPTOS Society Literature Contest Winners: First Place: [redacted] and Second Place: [redacted] Third Place: [redacted] Honorable Mention: [redacted] Honorable Mention: [redacted]

4f. (U//[redacted]) KRYPTOS Society 1999 Distinguished Members: [redacted], Phillip W. Dibben [redacted], R. Dale Shipp and A. Leslie Yoxall (Presentation Address by [redacted], President-Elect of the KRYPTOS Society)

5. (U) Community News

5a. (U//[redacted]) Applied Mathematics Program Graduation by [redacted], RSI

5b. (U) Mathematics Two Thousand Conference, January 24-28, 2000

5c. (U) Computer Network Exploitation Conference, March 6-8, 2000, Call for Abstracts

5d. (U//[redacted]) The CryptoMathematics Institute (CMI): Collecting Receipts for Computers by [redacted], Z

6. (U//[redacted]) Technical Article: [redacted] SCAMP '99 or "How I Spent My Summer Vacation" by [redacted]

7. (U) KRYPTOS Puzzle

7a. (U) New Puzzle: Annual KRYPTOS Kristmas Kwiz

7b. (U//[redacted]) Solution to Previous Puzzle: "Disemvoweled," by [redacted]

8. (U) Letter from the Editors

9. (U) Editorial Corner

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

//

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

[redacted]

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

1. (U//FOUO) PERSPECTIVE: Introductory Remarks at the Annual KRYPTOS Society Luncheon
by [redacted] President

(U//FOUO) As most of you know, NSA has been under enormous external scrutiny during the last year. In an era when our Agency has received a good deal of negative criticism, I would like to share with you some positive feedback from a member of the NSA Scientific and Advisory Board (NSASAB), former D/Director, Miss Ann Caracristi. Her words cut right to the heart of our career field--cryptanalysis.

(U) "Being on the NSASAB made me think again about why I have always enjoyed so much the company of these people who have always been the backbone of our business. In the past, I'm sure, I was delighted by the pure originality and eccentricity of so many of the 'characters' who played important roles insolving the 'impossible' problems. But, of course, bright people are always fun to be around. What is so special about 'cryptos'? I suspect it is that they are trained to be forthright and fearless in dealing with the problems at hand. They don't equivocate. Two plus two is four. Not ALMOST four. On the other hand, they know that there are still mysteries to be uncovered. They are receptive to new ideas and concepts. They are optimists. We know how tenacious a cryptanalyst must be and how important it is to have confidence in the validity of an attack. And, although they can be fiercely competitive, mathematicians have a habit of (maybe even a compulsion for) sharing and defending their ideas. And finally, these are people who frequently retain a charming touch of childlike wonder and appreciation for both the elegant and the absurd."

(U//FOUO) All of those that we are about to honor today reaffirm Miss Caracristi's words. It is with tremendous pride that [redacted] and I introduce the winners of our 1999 competitions to you.

(b)(3)-P.L. 86-36

---

2. (U) CALENDAR OF EVENTS

Jan 24-28 (U) Mathematics Two Thousand Conference (M2K)
(See article 5c.)

Jan 28 (U) KRYPTOS Kristimas Kwiz Solutions Due
(See article 6a.)

(U) PLAN AHEAD

Feb 2 (U) Sixth Annual Breakfast Affair for Newly Certified Cryptanalysts (BANCC)
(See article 3.)

Mar 6-8 (U) Computer Network Exploitation Conference
(See article 5.)

---

3. (U) Sixth Annual Breakfast Affair for Newly Certified Cryptanalysts (BANCC)

(U) Mark your calendars for the sixth annual BANCC:

Wednesday, February 2, 2000
8:00 to 10:00 a.m.

(U) Sponsored by the Cryptanalysis Career Panel and the KRYPTOS Society.

(U) Be on the lookout for more details of this popular event.

(U) Tickets will go on sale in January!

---

4. (U) KRYPTOS SOCIETY NEWS

4a. (U) KRYPTOS Society Election Results

(U//FOUO) The KRYPTOS Society is pleased to announce the winners of the 1999 Election. The newly elected officers are:

(b)(3)-P.L. 86-36

[redacted] President
President-Elect
Treasurer
Member-At-Large
Member-At-Large

Congratulations to you all.

4b. (U//FOUO) CSE KRYPTOS Election Results
by [redacted], Secretary, CSE Chapter of the KRYPTOS Society
For [redacted] 1999 President, CSE Chapter of the KRYPTOS Society

[redacted]

(U//FOUO) The CSE Chapter of the KRYPTOS Society is pleased to announce our officers for 2000:

President

President-Elect

Treasurer

Secretary

Congratulations to all new and returning officers.

4c. (U//FOUO) KRYPTOS Society Peter Jenks Award -- for [redacted] Z8

(Presentation Address by [redacted] President of the KRYPTOS Society)

(U)//FOUO) The Peter Jenks Award is intended to recognize service to the Cryptanalytic Community. It is presented jointly with the Cryptanalysis Career Panel. Peter Jenks himself was a powerful promoter both of cryptanalytic excellence and of suitable rewards for cryptanalytic achievement.

(U//FOUO) Throughout his career, [redacted] has demonstrated a deep and ongoing commitment to the cryptanalytic community through the performance of numerous community service activities and by serving in leadership roles in various cryptanalytic organizations. Dave has been an active member in the KRYPTOS Society and served as Program Committee Chair, President-Elect, and President in recent years. He has been a member of the Crypto-Mathematics Institute (CMI) and served as the Head Judge for one of the CMI literature contests. Dave was the first recipient of CMI's prestigious President's Award in 1978. In 1988 he was a judge for NSA's Cryptologic Literature Award. Always generous with his time, Dave also shared his broad expertise with the National Cryptologic School by serving on a board which performed an intensive review of the cryptanalysis curriculum. He has also served on the RSE Board of Governors, the SRC Advisory Group and the Crypto-Mathematics Program Board of Governors. During the late 1980's, Dave served the entire CA community as Chairman of the Cryptanalysis Career Panel. Under his guidance the Panel made major modifications and improvements to the CA certificaton process. The Professional Qualification Exam was completely revised to reflect the more modern cryptographies which were prevalent. This very active panel also instituted a change in the way CA papers were reviewed for certification. The result was a fairer grading system and a process which provided the analysts an opportunity to discuss their work with their reviewers.

(U//FOUO) Dave's professional contacts outside of NSA have always been impressive. He has maintained an active liaison with our "think tanks" at the Center for Communications Research. As a direct result, the CA community has benefitted tremendously. Dave has been equally adept in dealings with our Second Party partners and has been responsible for much of the synergy our community enjoys.

(U//FOUO) In the early 1990's, Dave was one of the pioneers in the development and the implementation of the Technical Track Program. As a member of the B Group Technical Career Advisory Board, he shared his career experiences, insights, and his time to help to develop the program. Later in his career, Dave served on the Operations Directorate's Technical Track Review Panels for both Mathematics and Cryptanalysis.

(U//FOUO) Dave's career can be characterized as distinctive, always finding him on the leading edge of technology. He thrives on challenge. As the first Chair of the Z Group Telecommunications Training Board, he provided the energy and focus for the community's transition to the network environment. He recognized early on that a fundamental understanding of new communications' structures was going to be critical to cryptanalytic success in the future. He gathered interested personnel, researched available commercial training, fought to get funding, and sponsored several courses to introduce the community to the emerging environment. It was his vision and drive that moved the corporation in the direction of expanding the training opportunities for current and future cryptanalysts.

(U//FOUO) Perhaps Dave's most significant contribution has been his forward thinking and his encouragement of the junior professionals, whom he has managed to personally recruit and motivate, to produce extraordinary technical achievements. He has an uncanny ability to attract excellent people, and motivate them to excel even beyond their personal expectations. This ability is a reflection of the high esteem with which he is held in the CA community. Dave's mentoring has always extended beyond his own organization and he provides technical direction and career guidance to a broad spectrum of the CA community. Colin Powell has said that "Perpetual optimism is a force multiplier. The ripple effect of a leader's enthusiasm and optimisim is awesome." Well, we all know how awesome our cryptanalytic workforce is. Much of that is due to the past and continuing efforts of this year's winner of the Peter Jenks Community Service Award--[redacted]

4d. (U//FOUO) KRYPTOS Society Norman Roberts Award -- for [redacted]

(Presentation Address by [redacted]

(b)(3)-P.L. 86-36

[redacted]

President-Elect of the KRYPTOS Society)

(U//FOUO) The Norman Roberts Award was established by the Cheltenham Chapter of KRYPTOS to honor the memory of our late colleague and friend. This award can be given annually (though not necessarily) and recognizes relatively junior individuals who are making an impact on our discipline in some of the same ways that Norman did. Thus, one of the criteria would be technical excellence--solving the hard problems and advancing the science by devising methods which apply to many problems. Now typically, Norman spread his ideas around by working in collaboration with another individual, by presenting his ideas in talks or in writing so that others could share in their development and learn. So it is equally important that the recipient of the Norman Roberts Award be a strong mentor, both to individuals and to the cryptanalytic community as an entity. Through his work, Norman showed a diversity of interests--working on many types of problems and frequently transferring methods developed on one type to a new problem. This establishes yet another characteristic that a candidate for this award should exhibit.

(b)(3)-P.L. 86-36

(U//FOUO) Receipt of the Norman Roberts Award is a GREAT and singular honor. [redacted] this year's honoree, is extremely deserving; he has all the hallmarks of a great technical leader; it would be hard to cite any other young member of our community who has had, so quickly, the extensive impact of [redacted]. Let me allude to some examples in an unclassified form which, I hope, will show the basis of these statements.

(U//FOUO) Words and their meanings are important. In technical fields, we can often see a reflection of the fact that technology has changed by observing how the definitions of words and phrases have developed. For example, the phrase "active attack" has been present in INFOSEC jargon for perhaps as long as 30 years. Over that time, nuances added to the original meaning of that phrase. About 10 years ago, that phrase took on added meaning and began to be more widely used. All of which signified that a major technological change was happening. The latest change in our lexicon involving that phrase has just happened and reflects a revolutionary change in our thinking, a change brought about by [redacted] most recent work. That work has added an important tool to the C Group evaluation arsenal and raises issues that [redacted] NSA's cryptographic designers, must now address upfront. Through these pioneering efforts, [redacted] has given an eye-opening lesson to the ISSO cryptographic community which is certain to impact the scope of future evaluations.

(b)(3)-P.L. 86-36

(U//FOUO) Each summer now, the Agency sponsors three events called SCAMP at which NSA technical people get together with academics and work very hard on some important, often fundamental, problems. These SCAMPs are held in La Jolla, California; Princeton, New Jersey; and Bowie, Maryland. [redacted] attended the 1997 Bowie SCAMP which addressed questions in a new, non-traditional area and during it, he fully developed a practical result. It was so impressive that then Deputy Director of CCS, [redacted] referred to it as "the best result to come out of SCAMP '97." So it was not a surprise that [redacted] was asked to brief the CIA on his work, as part of a CCS group describing SCAMP results.

(U//FOUO) After SCAMP, [redacted] made certain that the operational office responsible for this class of problem had all the help that they needed to actually make use of this result. He also gave a brilliant lecture to the NSA technical community explaining and demonstrating his new approach.

(b)(3)-P.L. 86-36

(U//FOUO) [redacted] and entered on board as a member of the C Development Program (now called the IDEP). [redacted] Jeff Zehe and [redacted] have all given stunning commentary on [redacted] accomplishments as an intern in their organizations. For example, when a previous D/DIR personally tasked the Barbershop to [redacted] continues to consult with folks in the Barbershop and this collaborative link that he maintains between SIGINT and INFOSEC is an important one for NSA with altogether too few parallels.

(b)(6)

(b)(3)-P.L. 86-36

(U//FOUO) During the past year, [redacted] has also contributed to a special, sensitive project. This work stands out for its technical content and for the thoroughness with which [redacted] pursued the right questions to their final answers. His initial charge was a simple review of the previous work done and was expected to have been routine. Nonetheless, [redacted] found relatively minor, technical errors. After correcting them and institutionalizing his corrections in software, he made a significant, purely cryptanalytic observation and that observation engendered a debate conducted at very senior levels about the appropriate corrective measures. Thus, [redacted] had strengthened the security posture of the USG when similar important applications occur in the future. Moreover, [redacted] was able to abstract the salient points, divorcing them from the sensitivity of the application, and his paper giving the essence of his analysis is available to the widest possible audience within NSA.

(U//FOUO) These are only a few examples of the positive effect that [redacted] has had on the science of cryptanalysis and cryptomathematics in C, and more broadly the Agency as a whole. Each example shows that [redacted] is an extremely gifted cryptomathematician;

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

that he can literally do it all. The consistent theme that runs through all the examples of his work is that as he develops or learns new technology, [redacted] shares it with his colleagues in such a way that they too will have an active role in its development. It is not a stretch to say that [redacted] stands out as a role model for us all in the way to conduct work in cryptomathematics and cryptanalysis.

(U//FOUO) It is with great pride that I introduce [redacted] the winner of the 1999 Norman Roberts Award. (b)(3)-P.L. 86-36

4e. (U//FOUO) KRYPTOS Society Literature Contest Winners:
First Place: [redacted]
Second Place:
Third Place:
Honorable Mention:
Honorable Mention:

(U) The judges in this year's KRYPTOS Society Literature Contest read 24 submissions, many of which were quite lengthy, and most of which were very well written and of substantial cryptologic importance. They asked us to extend our commendations to the authors, and commented on the difficulty of selecting only a few winners from the many worthy contributions. They have chosen to award, in addition to the three top prizes, honorable mention to two other excellent papers.

(U//FOUO) The authors of the two papers selected for honorable mention are both mathematicians, one an experienced analyst from GCHQ, the other a bright young intern from NSA.

(U//FOUO) The GCHQ winner, well known to cryptomathematicians for his many fine research contributions, is [redacted] cited this time for another theoretical paper, on a branch and bound approach to finding integer relations. [redacted]'s paper presents a new technique for solving a class of mathematical problems of interest to both NSA and GCHQ. In a field of research where relatively little is known about the complexity of the algorithms involved, the paper provides some vital first steps to understanding this complexity, and suggests several avenues for further research to refine these ideas. (b) (3)-P.L. 86-36

(U//FOUO) The other citation for honorable mention goes to a young man in NSA's Applied Mathematics Program (AMP), [redacted], for a beautifully written paper on a specific cryptographic problem of substantial intricacy. Also included is a brief history of a predecessor system. The judges applauded [redacted] writing style and understanding of several useful cryptographic techniques.

(U//FOUO) Our third prize goes to another GCHQ cryptomathematician, a young lady who has in her brief career won recognition for many successes, including the Norman Roberts Award. [redacted]'s new paper describes a diagnostic success arising from the so-called "new technologies," and shows what can be done by clever analysis in a complex situation. There were many withdrawals from blind alleys before her efforts were rewarded, and there is much for each of us to learn from reading the account of her adventure.

(U//FOUO) The second-place paper, authored by [redacted] another participant in the AMP, analyzes an American cryptographic process, and the improved understanding increases our confidence in the security of an algorithm. His final results include characteristics and properties of the function not previously observed, though it has been studied by many more experienced analysts. The judges appreciated his sophisticated use of very careful mathematical analysis in reaching interesting conclusions.

(C//SI) The paper judged the best in our Literature Contest is a very lengthy and remarkably comprehensive monograph by [redacted] who is in the Cryptologic Mathematician Program (CMP); [redacted] 207; and [redacted] also in the CMP; on a particular very popular [redacted]

4f. (U//FOUO) KRYPTOS Society 1999 Distinguished Members: [redacted] L. Phillip W. Dibben, Lowell K. Frazer, [redacted] R. Dale Shipp, and A. Leslie Yoxall
(Presentation Address by [redacted]
President-Elect of the KRYPTOS Society)

(b) (1)
(b) (3)-P.L. 86-36

(U//FOUO) "We can see so far because we are standing on the shoulders of giants..." I am no longer certain of whom to credit as the author of this or whether it is an exact quote. However, it is certainly true.

(U//FOUO) The question of who are the giants in any field of endeavor is always an interesting subject to consider and debate. As a subject, it is almost inexorably surrounded by controversy and differences of opinion. This year I had the honor of chairing the process which nominated those individuals who are being named Distinguished Members by KRYPTOS. After a review of "all" retired persons from the cryptanalytic career field, we attempted to weigh the contribution of each candidate against the standard of

(b) (3)-P.L. 86-36

[redacted]

"furthering the science of cryptanalysis." As a result of these deliberations, the Central Chapter of KRYPTOS is adding six new names to the roll of Distinguished Members. Each has contributed to cryptanalysis in a different way but in a manner consistent with the high standard of excellence which is represented by those elected to Distinguished Membership in the past. In addition, the Cheltenham Chapter is adding one new Distinguished Member. Without further ado, the seven names are: [redacted] Phillip W. Dibben, Lowell K. Frazer, [redacted] R. Dale Shipp, and A. Leslie Yoxall.

(b)(3)-P.L. 86-36

(U//FOUO) [redacted]

(b)(3)-P.L. 86-36

[redacted]

(U//FOUO) Throughout his career, [redacted] was a technical whiz with a unique sense of humor. His genius was the ability to understand the latest mathematical technology and make it work on a specific problem. [redacted]

(U//FOUO) In A5, [redacted] worked on almost all of the important problems, but I will always associate him with working on my very favorite one. During some particularly heady times in A5 which spun off from an earlier discovery by [redacted] and which were characterized by brilliant insights from [redacted] and others, [redacted] was a leader and a technical genius. I believe that [redacted] never ruled out any problem as being 'a priori', too hard to solve, no matter how outlandish that may have seemed. [redacted] even had the chutzpah to champion [redacted] In the end, the entire effort that I have alluded to was a resounding success. Even though it was the product of many great minds, many more than in my short list, I associate [redacted] with it more than anyone else. [redacted] was awarded the Exceptional Civilian Service Medal for his work in A5.

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36
(b) (6)

(U//FOUO) [redacted] was a worthy past President of KRYPTOS; a mentor to junior people throughout his career; always willing to share his ideas in such a way that the recipient felt lifted-up and not put-down. [redacted] was co-founder of the first pod, working on pods up to his retirement; much of the success of the pod concept is due to his direction and enthusiasm. He is the recipient (the first, I think) of the newly established "Director's Distinguished Service Medal."

(b)(3)-P.L. 86-36

(U//FOUO) I feel fortunate to have known [redacted] throughout our careers as NSA mathematicians and cryptanalysts. It is with great pride that I give you [redacted] Distinguished Member.

(U//FOUO) Phil Dibben

(U//FOUO) I have been unable to find out much factual information about Phil's early career up to just quite recently (about the same time that I learned that Phil knows how to say "Grand Canyon" in [redacted]

1980, Phil had risen to Chief, A5. Now Phil, I apologize for any inaccuracies in this timeline; there were last minute changes. However, any infomational gap did not in any way hinder the nominating committee. To a person, they all had direct experience in working in, (or in close partnership with) A5 and believed that A5 was a tremendously successful organization--sucessful beyond any reasonable expectation when one understands how hard the problems that A5 confronted were. Several on the committee were fortunate to have directly observed the leadership that Phil supplied and how it made success a real possibility.

(U//FOUO) Moreover, during the 1960's, the technology underlying was changing in a radical way. This made it necessary for A5 to also change, if it was to have any hope of success. It is by no means a given that management would understand that this technological change implied that there was a need to apply mathematical methods that had never been used before; that there was a need for hiring additional mathematicians into A5 would bring new mathematical insights along with them; and that there was a need for additional computing horsepower at both the frontend processing and at the analytic end. Phil realized this and vigorously fought for what his cryptanalysts

(b) (3)-P.L. 86-36

[redacted]

needed. Moreover, he also knew how to keep the best of the "old-technology-AS" and foster the development of analysts working these problems for the eventual transitions that they would have to make.

(U//FOUO) I an happy to present Phillip W. Dibben, Distinguished Member.

(U//FOUO) Jim Frazer

(U//FOUO) In 1939, Jim graduated from high school at the age of 14 and started attending Indiana University. He received his bachelor's degree in mathematics but the war interrupted before he could finish his master's. He returned after the war and finished up his master's, then received his Ph.D. in 1951, all from Indiana University. Immediately after getting his degree Jim went to work for the government.

(U//FOUO) The nineteen scholarly papers in the C Group Library that Jim has authored or co-authored testify to the strength of his technical contributions. These papers range from evaluations of specific cryptographic algorithms, to papers on general attacks applicable to many algorithms. In this latter category is a method called the Gang Attack which he invented for a particular problem, but which has much broader applicability. He was also a pioneer in applying approximate methods. Jim wrote a monograph in the P1 Monograph Series which introduced many of us, including myself, to an area of technology that was the mainstay of our business, both INFOSEC and SIGINT, for thirty years. His monograph, which gave the COMSEC spin on that subject, predated and was a companion paper to the classic [redacted] treatise on the same subject. Together with [redacted] Jim is credited with establishing a formal high-grade "Cryptographic Standard." Together with the [redacted] of Costing, this put (and has kept up to the present day) the evaluation of the cryptography used to protect classified government information on a rigorous, scientific basis.

(b)(3)-P.L. 86-36

(U//FOUO) As a manager, Jim is generally credited with bringing mathematics to bear on the process that evaluates cryptography. Jim recruited many of the mathematicians who work on evaluations today. He insisted that such evaluations conform to a high standard of rigor and defended these "high standards" from being eroded by operational or market expediency. If you understand the difference between COMSEC and INFOSEC and that the latter is a much better thing to have, then you will appreciate the fact that Jim was a big advocate for INFOSEC before that term became popular, leading his organization in the direction of INFOSEC. All of this and ... he was a strong supporter of giving his analysts the computing tools that they needed.

(b) (6)

(U//FOUO) Jim is now the CEO of Information Security Systems Incorporated, the company that he started in 1985 after retiring from NSA as Chief S6. He has sons, Ron and Doug, working with him along with about 25 retired NSA engineers and scientists.

(U//FOUO) The founder of Modern Cryptographic Evaluation and now Distinguished Member of KRYPTOS, here is Jim Frazer.

(b)(3)-P.L. 86-36

(U//FOUO) [redacted]

(U//FOUO) In Dale Shipp's introduction which is yet to come, I mention an event whose "timing coincided with the arrival of the 6600 and IDASYS." Involved with this event was a program which might have been named MEGAWEAVE and which was written for the 6400 by the late Jerry Mitchell at IDA in Princeton. Jerry had the writing of this program in mind for some time but became really motivated when a new, large dataset arrived from NSA. Dennis was largely responsible for this new data. Later as analytic discoveries began to be made, [redacted] would supply either a larger data set or make some improvements in the quality of that data. It frequently seemed that breakthroughs on that problem were brought about more by the "better" data than by some brilliant analytic insight. Dennis maintained and sharpened these skills that he used to improve the data and the demand for these services from him persisted throughout his career.

(U//FOUO) [redacted]

(b)(3)-P.L. 86-36

skills in a more direct way to cryptanalysis and cryptanalytic questions. Later in his career, he and [redacted] with some contributions from [redacted] solved a challenging cryptanalytic problem, albeit of only minor operational importance. Initially brought in to "improve the data," he could not stay away from the core of the problem and in the end, contributed big time to the solution. Both the core problem and data improvement involved the same type of problem solving, patching together the big picture from incomplete and misleading shards of evidence. "Working for [redacted] in the 1980's and with [redacted] continued to make contributions to diagnosis and later showed considerable interest and ability at understanding hardware.

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(U//FOUO) [redacted] works so quietly on a problem, and even though he

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

[redacted]

may have solved or contributed to its solution in a big way, it would be easy to overlook him and miss the value of his contributions to cryptanalysis. I am proud that KRYPTOS did not do that. I am sorry that [redacted] could not be with us today.

(U//FOUO) [redacted] (b)(3)-P.L. 86-36

(U//FOUO) [redacted]

known as the author of a succession of programs to solve this problem, each of which was viewed in its time as the very best. Each of these instantions surpassed its predecessor either by exploring the architecture of the computer in some better way or by employing the latest, and often highly sophisticated, mathematical algorithm. Over the course of his involvement with this problem, the total increase in speed and our ability to handle large problems was truly astounding and enabled the establishment of a new branch of "crypto-" science. Later, [redacted] took on another cryptanalytic algorithm and had a similar degree of success.

[redacted]

(U//FOUO) During his career, [redacted] has been honored with a Meritorius Civilian Service Award, several Senior Technical Achievement Awards and the Cryptologic Literature Award. [redacted] is very proud of this last award and of his tome on Cryptanalytic Attacks that earned it. Throughout his career, [redacted] has championed advances in cryptanalytic computing both by pushing for improvement to hardware platforms and by encouraging the use of the most effective software algorithms. In addition to promoting and effecting improvements in computing, [redacted] has solved or made contributions towards a number of specific cryptanalytic problems. That brief remark give an important part of [redacted] career short shrift and does not do justice to a strong record of accomplishments in that arena. I give you [redacted]

(b)(3)-P.L. 86-36

(b)(6)

(U//FOUO) Dale Shipp

(U//FOUO) [redacted] Dale came to NSA as an Army 1st Lieutenant in 1967 to work in A54 (actually A58). He together with Nick Howard, [redacted] Al Verbits, and Leslie Sage worked for Jim Bates in a small research branch. Later promoted to captain, and in 1969 promoted to civilian at NSA, Dale continued to work in A5. During this period (I am guessing 1968), Dale contributed to a major success whose timing coincided with the arrival of the [redacted]. In 1972, Dale took a turn at GCHQ. He returned to work in A5 in 1975, attending a West Coast SCAMP a few years later. He was Chief, B42 from 1980 to 1984 at which time he did a tour as C/Chief G2 and Chief S61 (G4 now) under the auspices of the SCEDP. On this latter tour, Dale had the opportunity for technical work and that experience convinced him to rejoin the technical track. From 1985 [redacted] Dale addressed diagnosis in A5 under the auspices of P1 and later as a senior technical person in Z2.

(b)(3)-P.L. 86-36

(U//FOUO) Dale is credited with inventing several analytic techniques (one of which is known as a method of [redacted] with writing several papers on topics of fundamental importance to cryptanalysis (one of which appeared in the Special Issue of the Technical Journal), and for being a career-long champion of diagnosis (both as a manager and in terms of his technical success). Dale is also recognized for serving with distinction in INFOSEC. Dale has received the Execptional Civilian Service Medal and was in the group of 10 who received the first Superior Technical Award. Here is Dale Shipp.

(U//FOUO) Leslie Yoxall

(U//FOUO) Leslie graduated from Cambridge University in the 1930's and became a Research Student finishing his Ph.D. at the beginning of World War II. After a period of teaching, he was interviewed by Hugh Alexander and Alan Turing to work on Naval ENIGMA and joined Hut 8 (as the buildings at Bletchley were denoted) on 1 May 1941, where he took part in daily breaking and solved the Offizier problem. In the latter part of the War, he worked on the Japanese Naval Machine JADE.

(U//FOUO) He stayed at GCHQ at the end of the War and spent the rest of his career in H Division with two tours in the U.S., finishing up as H1 (with particular concern for special projects) and Deputy to Hugh Denham. In the early years he was responsible for the recruitment of mathematicians and other specialists, and for mathematical and cryptanalytic training. Throughout his career he helped plan, prepare and conduct training courses, continuing as a

(b)(3)-P.L. 86-36

[redacted]

consultant until July 1997.

(U//[redacted]) During (and since) his two tours in the U.S., Leslie, and his wife Doris, helped to strengthen UK/UK relations. Following his first term as H Liaison Officer (1959-63), Dr. Louis W. Tordella, D/DIRNSA wrote to the then Director, GCHQ, Sir Clive Loehnis: "His superior technical competence and analytic insight have served as a stimulus to everyone with whom he came in contact. His engaging personality, diplomacy and tact have endeared him to us all."

(U//[redacted]) When Leslie retired in July 1977, the Director's farewell letter paid tribute to his work: "Some of your achievements are known to very few of us (and none the less valued for that), but other things you have done, like the help you have been to the work of innumerable people, are widely known and respected.", and "you can regard the continued existence of our special relationship with the Americans as owing much to your efforts."

(U//[redacted]) Since retiring from GCHQ, Leslie has become well known locally and further afield as a teacher of mathematics. He is a Distinguished Member of the CMI and a Fellow of the Institute of Mathematics and its Applications. Accepting on behalf of Leslie is Peter Hyland.

---

5. (U) COMMUNITY NEWS

5a. (U//[redacted]) Applied Mathematics Program Graduation
by [redacted] R51

(b)(3)-P.L. 86-36

(U) The Applied Mathematics Program (AMP) held a graduation ceremony for its first class on September 13, 1999. Over the past three years these mathematicians have faced the challenges posed by the revolution in communications technology. The problems they have addressed in many of their tours disregard the traditional boundaries between mathematics, computer science, and engineering, and reach new levels of difficulty each day. In addition, these mathematicians have been exposed to the "traditional" work done by mathematicians in the development of the science of cryptology, and have been successful in that arena also. But the majority of the members of the AMP Class of 1999 have chosen to continue their work on problems raised by the technology explosion by choosing offices where they can apply their exceptional versatility, profound creative energy, and relentless drive to these exciting new problem opportunities.

(U//[redacted]) The offices where the first graduates will be working are as follows:

[redacted]

5b.(U) Mathematics Two Thousand Conference, January 24-28, 2000

(U) The Mathematics Two Thousand Conference (M2k) is scheduled for January 24-28, 2000. This large internal classified math conference will be held directly following the Joint Mathematics meetings to be held in Washington, D.C. in January 2000. The conference will be modeled after the joint meetings in style, and will include participation from the entire extended cryptomath/CA community (IDA/Second Party partners/SCAMP participants/etc.).

(U) The format for the conference is as follows. There will be a two-hour session each morning, in Friedman auditorium, consisting of accessible talks of interest to the entire community. An invited plenary talk will be given each day in Friedman at 1600. The intervening period each day will be devoted to short courses, typically lasting 2-4 hours and possibly spread over 2 days, and special sessions. It is planned that TD credit will be offered for some of these courses through the NCS. Special sessions will also mostly last between 2-4 hours (a few will be longer) and be typically composed of technical talks, rump sessions, and panel discussions. To see the current list of short courses and special sessions check the M2K webpage at: [redacted]

(b)(3)-P.L. 86-36

(U) Abstracts of the technical and plenary talks will be available from a site on the CA web as they become available. Attendees from Second Parties will not be able to access the CA site; however, any information will be mirrored to the appropriate Second Party sites.

[redacted]

(U//FOUO) Advance registration is strongly recommended for both the short courses and special sessions. Registration is being handled over the NSA Web, thru the M2K Web page. Second Party attendees and those unable to reach the M2K webpage can register by e-mail through

(U) The CMI and the KRYPTOS Society are sponsoring some social events during M2K. Tentatively, the following two events are planned. One, an evening gathering on Sunday, January 23rd at some establishment in Columbia. Two, an afternoon "classified mixer" on Monday, January 24th in Z2 spaces. Look for updated details in the coming weeks on the M2K homepage.

(b)(3)-P.L. 86-36

5c. (U) Computer Network Exploitation Conference, March 6-8, 2000: Call for Abstracts

(TS//SI) Computer Network Exploitation (CNE) has become one of the primary areas of interest of both the offensive and defensive portions of NSA. To provide an opportunity for exchanges among professionals throughout the community, a technical conference on CNE will be held March 6-8, 2000 at the Center for Computing Sciences (CCS) in Bowie, Maryland. Attendance will be limited to NSA, CIA, and IDA employees. Topics may be drawn from any subject related to network exploitation including:

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) We are calling for speakers to notify any of the POC's below of their intent to give a talk at this conference. Please send the following information:

Name
Office
Telephone number
SID
Length of talk (20 - 30 minutes preferred)
Brief description of talk

(U) The deadlines for submissions are:

Nov 19: Notification of Intent to Speak
Dec 4: Short (1-3 pages) abstract due
Jan 7: Speakers notified of selection
Feb 4: Extended (1-6 pages) abstract due

(U//FOUO) POC's:

5d. (U//FOUO) The CryptoMathematics Institute (CMI): Collecting Receipts for Computers
by

(b) (3)-P.L. 86-36

(U) The CryptoMathematics Institute (CMI) is once again sponsoring the Ruth Parker Eason School in Millersville, Md. with regard to the local grocery stores' (Giant, Safeway, Metro, etc.) cash register receipts programs. Cash register receipts may be exchanged for computers and other useful equipment.

(U) The Ruth Parker Eason School is a public school for children (aged 3-20) with special needs. Many are multiple-handicapped and require specialized equipment to facilitate their education. Computers have been an important part of the education process and the school adapts them for use by even the most physically handicapped child.

(U) In addition to the computers, the grocery stores allow for the purchase of other specialized equipment in exchange for the receipts --much of which would not otherwise be paid for by the county. An example is a piece of equipment that allows a child, who is otherwise unable to stand, to be supported--so that he/she can more easily take part in some of the school's activities. Without the help of this program, this small school would have to fund ~ $2500 for each of these devices.

(U) Last year CMI collected almost $50,000 worth of receipts for this school and was honored with a wooden plaque. I was also fortunate enough to be offered an in-depth tour of the school by the principal, in appreciation for NSA's support. It was very inspirational.

(U) If you don't have kids, your kids are all grown up, or you are fortunate enough to have kids in schools with lesser needs, please consider donating your receipts to this cause.

(U//FOUO) If you choose to do this, please send them to me, on tour as Z rep DO Business Results Center 3C157, periodically and I will add them up, and assure that they are delivered to the school. (At Safeway, you now have to register your Safeway card at the customer service counter in the store in order to

have the totals credited to this school or to any school of your choice.)

(U//~~FOUO~~) If you'd like to put a box out in your work area (please mark it as being for the school so people will be clear on who the receipts are for), that would also be great! If you e-mail me [redacted], I'll even make the box :') and pick up the receipts periodically.

(U) Thank you very much for your consideration.

//

(b)(1)
(b)(3)-P.L. 86-36

6. (~~TS//SI~~) TECHNICAL ARTICLE: [redacted] SCAMP 199 or "How I Spent My Summer Vacation"
by: [redacted]

(~~TS//SI~~) This past summer's SCAMPs at IDA/CCS Princeton and at IDA/CCS-Bowie both were dedicated, in part, to work on compartmented projects for the [redacted] Program. This was novel in the sense that the compartment for this clearance, [redacted] now covered by [redacted] has rarely been given to researchers for such an effort before. Of course, you're probably wondering what I'm going to say in this article since the work was for a compartmented program. Well, many of the techniques we use (especially the "crypt-like processing" attacks/algorithms) do not give away the nature of exactly how we acquire our data nor the location/identity of our targets, which is mainly what the compartments protect. So I'll be able to write about more *than* you might think possible.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) As with all similar undertakings, there were some hurdles to overcome first. Determining the problems to be worked on was the first priority, BUT, getting the appropriate data released to be seen at SCAMP was potentially an insurmountable hurdle. So, we (Z71) had to convince our customers in DO (M & W) that it would be good for them to let us release their data. Fortunately, the offices that had the vision/foresight to allow this sharing of data are now thrilled with the progress we have made on some of the most difficult problems involved in the successful production of intelligence from their targets.

(~~TS//SI~~) There were four main problems proposed for research at the SCAMPs (at Bowie and at Princeton), [redacted] In order to maintain a certain amount of vagueness that will help keep this article from being compartmented, I'll tell you about the work that was done without correlating it to the covernames. The work was divided into the [redacted] SCAMP.

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U//FOUO) This year's SCAMP was, from ZTI's standpoint, definitely a success, and hopefully, the starting point for a continuing fruitful relationship between our program and the researchers at the IDA's and other organizations. Plans to continue most of this work are already well underway and there are many related projects just waiting to be followed up on! If you're interested in working in this area, please contact me, [redacted]

(b)(3)-P.L. 86-36

//

7. (U) KRYPTOS PUZZLE

7a. (U) New Puzzle: 1999 KRYPTOS Kristmas Kwiz

(U//FOUO) Answers are due COB on January 28, 2000. Two changes from previous years are that we are giving away prizes to the winning team, and teams are limited to 4 or fewer members in order to win a prize. If you have any questions regarding this Kwiz, please contact the following people: [redacted]

Please send solutions to this puzzle to [redacted]

(b)(3)-P.L. 86-36

(U//FOUO) This year, [redacted] have been joined by [redacted] to create the 1999 "KRYPTOS Kristmas Kwiz." As usual, some questions are more difficult than others, so each has an associated Warp Factor. For factors greater than 1, points may be awarded for a nearly-correct answer or even a gallant effort, so give an answer even if you're not sure. And if your answer is better than ours, you may receive bonus points. The Kwiz is designed to be quite hard (in places), and some questions may be impossible thanks to [redacted] Brainstretch, [redacted] Overwarp or [redacted] Wisprint (though we have tried our best to avoid these!), so do enter the competition even if you haven't completed all the questions.

(U) Webster's Dictionary will be taken as the authority for what constitutes a "word": it must appear as an entry therein. Unless otherwise stated, an entry that is a proper noun or that includes punctuation (hyphen or apostrophe) does not constitute a "word". If your answer includes an obscure word which is not in Webster's, but in some other common dictionary, you must tell us which.

(U) We accept entries from individuals or from teams, but we would like to suggest that a team comprise no more than 4 members.

(U//FOUO) NSA'ers should e-mail responses to clbeannsa. Those at GCHQ should follow their own instructions. The names of the winner(s) and all contestants who received a score greater than zero will be published in an upcoming _Tales of the KRYPT_. The deadline for responding is COB Friday, January 28, 2000. This year the winner(s) will receive a FABULOUS prize (a KRYPTOS mug or glass!).

(U) So, good luck, and have fun!

(U) 1. Give two words that have the same pronunciation but have no letters in common. (1)

(U) 2. Where does PONY fit in the following list (read left to right, line by line):

BONE	HILL	REST	PRINCIPLE	KEEPER	DRIVE	SAINT
BUFFALO	LAW	CASTER	CHER	STROKE	ENTER	PEN
FLUENT	EVEN	PIP	CAPE	MARKET	PAPER	DIRTY
CHOICE	WALKER	SLOPPY	QUESTION	NAIL	REVENGE	NET
BALL	RAZOR	INTER	BOX	DISEASE	WIT	BLUE
LOT	CONSTANT	WEEPER	STRESS	RIFF	SIMPLE	PLANT
ON	LAZY	THING	OFF	RING	AVER	MOTHER

(5)

(U) 3. And, reading the same way, where does '55' fit in the following list:

8	58	1993	44	1	1700	1994
2000	3	1	1875	1752	18	3
5	6	9	5	1923	2	2
1587	1582	14	1873	3	13	8
6	80	93	1997	46	1	1
15	1995	70	94	1939	1996	45
6	34	7	12	7	12	1998
2	92	4	1967	5	2	

(5)

(b)(3)-P.L. 86-36

[redacted]

(U) 4. Which is the odd man out:

a) BEGGAR, BOXCAR, DELIVER, HARDWARE, LITIGATION, MOLECULE, SCOWL, SEVERAL, VOLATILE (1)
b) BAIT, BALL, BIRD, GUARD, JACK, LEG, LIST (1)
c) BODY, HOTEL, KNIFE, RELAXING, STATELY, TROUBLES, UNGRATEFUL WRINKLE (1)
d) ARSENAL, CARAFE, CIPHER, COTTON, IDEA, MAGAZINE, MATTRESS, MONSOON, SOFA, SYRUP (1)
e) CASTLE, DEATH, HARBOUR, IDEA, LITTLE, RECREATION, TYPE, WRONG (1)

(U) 5. This limerick has a different 5-letter word missing from each line. What are the missing words?

A man from the East, name of -----,
Would ----- give people red roses,
But he had an odd -----,
A strange ----- glare,
Which is why they would -----, one supposes. (1)

(U) 6. Come up with a (not-too-contrived) sentence containing the longest possible sequence of two-letter words. The words need not all be different, commas/semicolons are allowed if necessary (though quotation marks are not) and the sentence can begin and end with non-2-letter words. (1)

(U) 7. Identify the theme: to the English, it's only 40; to the French the first is 2; to the Germans the second is 8; to the Russians it doesn't exist. (1)

(U) 8. Which word could follow:

a) LACING, SCARED, COPING, TAMERS, CANONS, DENTED (1)
b) COMA, BATCH, DANCER, WARRANTED, SCARE, INFEST, GARDEN, SHRED, FIORD (1)
c) HONOUR, EXUDE, STORIES, REQUITAL, QUINCE, EXIST, PESTER, TOUCHING (1)
d) ADDS, ICE, CROP, PECAN, DON, MILLS, LATEX, SULK (1)
e) ELOPE, BUG, ENTER, REIN, LATE, OUT, SUCKER, PLOUGHS (1)
f) FIN, CAR, CON, CAN, IMP, OUT, BUD, WAS, OFF, RAM, FIP (1)
g) AMAZED, BRAYING, CRUXES, DROWNED, ELEVEN, FLOUTED, GRATES, HESSIAN, INURED (1)
h) PHARAOHS, DOUBT, SCISSORS, HANDKERCHIEF, YEOMEN, HALFPENNY, GNAT (1)
i) BE, BEAD, CEDE, DRAB, FACING, ILEUM, NATRIUM (2)
j) CHAIN, RIBBON, PRECIPICE, ADEQUATE, EAR, REFUSE, WEIGHTY, SHRUGGED, ACHIEVE, BEJEWELLED, PICKAXE, SMELLY (2)
k) OTHER, UTTER, PITFALL, CHUFFING, PROOFS, CONCESSION, SURPRISED, COMPREHEND (2)
l) INCH, INGOT, INSERT, INFERIOR, INCENTIVE, INDISPOSITION, INSENSITIVE, INTERMITTENT (2)

(U) 9. What is the longest word (of length n) from which letters can be dropped, one by one, in the order of your choice, to form words of length (n-1), (n-2) ... 2, 1
(e.g. DREAM - DRAM - RAM - AM - A)? (1)

(U) 10. Below are seven cryptic crossword clues. They do not contain a definition part, but all seven answers are related. There is no indication of the lengths of the answers, but again all conform to a pattern. The numbers following the clues are pointers to individual letters, which spell out an eighth member of the group.

a) Liquid metal reservoirs (3)
b) Greek one - stretch out (4)
c) Male beast, perhaps (4)
d) Extremely able junior hospital doctor, we hear (5)
e) Film certificate - sounds like a log cabin (5)
f) Civil Service, supporting one who relaxes (7)
g) Return computer - there are white specks on the screen (4)

What is the eighth member? Provide a cryptic clue. (2)

(U) 11. What is the longest word in which each consecutive group of n letters, in the order in which they appear, spells out a word [e.g. for n = 3, CARED gives CAR, ARE, RED]. Solve for:

a) n = 3;
b) n = 4;
c) n = 5. (3)

(U) 12. Each of the following lists leads to a second list, entry by entry, which leads to a third list, which leads to a fourth list, and this last list is in alphabetical order. What are the final lists?

a) GODS, VASE, GROWN, STAPLER, EARTHY, DIET, CANED, SERVE, SADDLER, SNAP, BLOTS, PLACER, PRIESTS (2)
b) BIRDWATCHER, BOMBING, BEEF STEW, DAGGER, BROAD-BRIMMED HAT, OPENNESS, DEAD END, OPEN PIE, GRIEVANCE OFFICIAL, DRUMBEAT, PAPER-FOLDING (2)

(U) 13. In the following, what does the "?" stand for?

UNITED KINGDOM	3435
AUSTRALIA	794
UNITED STATES OF AMERICA	3486
NEW ZEALAND	?
CANADA	16

(1)

(b)(3)-P.L. 86-36

(U) 14. Which sequence is the odd one out and why?

(4 8 11 13), (9 18 7 2), (16 13 1 19 8), (20 18 9 7 8),
(4 12 7 15 9 8), (7 1 15 20 8 19), (10 1 5 14 8 18),
(13 1 16 7 11 17), (16 1 9 19 11 20), (7 3 18 12 6 1 9) (1)

(U) 15. A recent competition asked for the best approximation of the form a/b to pi which used the digits 0-9 once and once only. The answer turned out to be: 85910/27346.
If we allow all basic arithmetic operations (*, -, /, +, ! and sqrt), decimal points, exponent (^), recurring and parentheses, but still insist that the digits 0-9 are used once and once only, can you find a better approximation? (1)

(U) 16. Out of all the 10-digit numbers that can be formed using each of the digits 0-9 once and once only, each of the following has a unique property. What are they?

a) 3816547290 (1)
b) 8549176320 (1)

(U) 17. What is the next matrix in this series?

(10 2 11) (12 12 3) (5 13 14) (16 7 14) (15 18 11) (13 16 20)
(19 36 1) (10 88 2) (10 40 2) (8 10 3) (5 16 4) (12 56 4)
(11 4 7) (18 1 17) (25 8 18) (16 5 12) (20 2 23) (15 9 21)
(3)

(U) 18. What do the following words have in common (apart from their lengths)?
1
a) ART, DOT, HAT, LOW, NAP, PAR, THE, WIN (1)
b) ANT, BRA, BUD, CAR, MAD, PAR, RIG, VIE, WAR (1)
c) ART, BEN, COP, DOT, FIR, HIS, JOY, LUX (1)
d) BEE, BRA, COP, HAY, MEN, PAL, PRO, RIM, WAG (1)
e) AND, BUR, EAT, ETH, GUY, RIM, WAG, WAN (1)
f) BUD, BUR, MAD, NAP, PAL, PAR, WAR, YAM (1)
g) ADD, CHA, DUD, END, ITS, OHM, RHO, TOR (1)
h) ART, BRA, BUD, BUR, COP, DOT, MAD, NAP, PAL, RIM, WAG, WAR (1)

(U) 19. In each of the following sets, the words preceding the colon share a common property, which is not shared by the word after the colon. What are the properties?

a) ABDICATING, BOWING, FATTER, PANTS, QUIRE, STOP: ABSENTEE (1)
b) CROCKERY, PORPOISE, RECIPE, STOCKPOT, STORY, TRICKY: SICKLE (1)
c) BLACKENED, DEFACING, FREIGHT, HIGHJACK, POLICEMAN, REQUEST, OVERTURNS: CERTAINLY (1)
d) ERROR, OUTER, PITY, QUIET, TORQUE, WRITER: FLASH (1)
e) BENZENE, BETWEEN, COLOURFUL, CRUX, FOIL, FRILL, GAD, JAMMY, KNEE, PAMPAS, VAMP, WHEEZE: GASEOUS (2)

(U) 20. What links:

a) colon, mobile, natal, nice, reading, tangier? (1)
b) the Roman Emperor Titus, Pope John IX, Archbishop Langfranc, Pedro the Cruel, Ferdinand Magellan, Li Yu, William Hogarth, Johann Strauss the Elder, George V? (1)
c) GARRISON, PORK, FIERCE, GIANT, HARES, TART, HOOKER? (1)
d) 100151100, 50151500, 1000110001100, 5151500? (1)
e) BRA, CARE, MILLIONAIRE, NEEDLE, PRINCE, TIMELINE (1)
f) 10, 190, 2766, 57005, 11325150, 14613198, 16435934? (1)
g) BUTCHERS, DIVER, HANDY, HARLEM, LARGE? (1)

(U) 21. Tidying up the other day I came across an old shopping list that I wrote out for a friend of mine who was poorly last Christmas. What was his name?

Pizza	Eggs	Rioja	Figs	Orange juice
Razor	Mixed nuts	Frying steak	Rusks	Emery boards
Quiche	Unsweetened squash	Expectorant	Nectarines	Cabbage
Yoghurt	Coffee	Oven chips	Underwear	Newspaper
TV guide				

(1)

(U) 22. The following were all of a kind and then mutated slightly:
AMENITY, CARAFE, ELEGANT, GLACIER, LEGENDARY, ROMANCES, SARCASTIC, SNAKEPIT, STAIRS, TIARA, THOUSAND, TRIBAL, WARDEN.
Where were they? (1)

(U) 23. The game of HANGMAN begins by an opponent choosing a word and telling you the number of letters in the word. You then try to deduce the word by guessing at the letters it contains. After each guess your opponent tells you whether the letter occurs in the word and, if so, where; if the letter does not occur in the word you lose a life. Upon the loss of your 7th life, you 'die' and lose the game; if you've guessed all the letters in the word before then, you've won.

(U) Normally, the results of the past guesses guide the future guesses. However, in the game of DUMB HANGMAN the guesses are the letters a, b, c, ... until the game ends. Which word could an opponent choose to maximize the number of guesses before you:

a) win; (1)
b) 'die'? (1)

(U) 24. Rene's 40 is equivalent to Anders' 50, Gabriel's 122, Sir William's 323 and William's 582 (approximately), while Anders' 20 is equivalent to Gabriel's 68 and Sir William's 293. What is Sir

(b)(3)-P.L. 86-36

William's surname? (1)

(U) 25. In a TV quiz show, children are asked to choose one of two possible answers to each of four questions: the first letters of the 8 possible answers are different. The first letters of the right answers spell out a word. Find 4 pairs of letters which give rise to the maximum number of 4-letter words (e.g. D/P A/O L/T E/S give DALE, DATE, DOLE, DOTE, DOTS, PALE...). (1)

(U) 26. Richmal Crompton, Johanna Spyri, Lewis Carroll, Wilbert Awdry, Vladimir Nabokov, Alexander Solzhenitsyn, Arthur Conan Doyle, Rudyard Kipling, Benjamin Disraeli, Harriet Beecher Stowe, Henry Wadsworth Longfellow, Dean Farrar, Joyce Lankester Brisley? (1)

(U) 27. What connects the numbers 12496, 14264, 14288, 14536, 15472? (1)

(U) 28. Solve:

a) 11 = S of a H
b) 12 = D in a G
c) 95 = T of ML
d) 1936 = FFS (2)

(U) 29. If 1/9 = .14, and 1/8 = .16, what does 1/6 equal? (1)

(U) 30. I have a torn piece of paper that shows some results of an international soccer tournament. The readable scores were:

GROUP 1				GROUP 2			
ENGLAND	4	GERMANY	4	LIBYA	1	VIETNAM	2
GREECE	5	ITALY	3	HUNGARY	3	INDIA	4
RUSSIA	11	ISRAEL	4	SCOTLAND	2	YEMEN	3
SPAIN	5	WALES	?	GABON	3	ALBANIA	?

GROUP 3				GROUP 4			
BULGARIA	3	CHINA	8	DJIBOUTI	0	CHAD	1
USA	6	ROMANIA	3	TOGO	0	EGYPT	2
PANAMA	6	MOROCCO	6	DENMARK	1	PERU	2
IRAN	4	FINLAND	?	CAMEROON	0	LAOS	?

GROUP 5				GROUP 6			
JAPAN	9	AUSTRIA	1	SINGAPORE	0	KIRIBATI	2
MALTA	1	BELGIUM	1	MALDIVES	4	ZAMBIA	0
KENYA	3	TURKEY	2	GHANA	0	NIGERIA	2
NORWAY	1	HOLLAND	?	ZIMBABWE	2	SRI LANKA	?

GROUP 7				GROUP 8			
QATAR	3	IRAQ	2	UZBEKISTAN	4	MOLDOVA	3
PARAGUAY	5	SWEDEN	1	ARMENIA	2	GEORGIA	3
SOMALIA	5	CYPRUS	2	AZERBAIJAN	3	TAJIKISTAN	3
JORDAN	2	AUSTRALIA	?	BELARUS	2	UKRAINE	?

(U) France was disqualified from Group 1. No Group 2 or 3 team has ever failed to score. Group 4 is generally low scoring. Groups 5 and 6 each have a limited number of qualifying teams. Greece is the only country never to have scored in a Group 7 match. Most teams in Group 8 score. Can you supply the missing scores? (8)

(U) 31. In a recent psychometric test, I was asked to associate the words BIRD, CAST, CAUP [sic], DOTS, FILM, PILL and WITH with the colours of the rainbow. What colour should I have chosen for each word? (1)

(U) 32. Complete:

a) if PELICAN=9, BEAR=25 and BADGER=30, what is 40? (1)
b) if C=6, S=16 and Y=39, what is 92? (1)
c) if JANE=23, MARY=30, ANNE=32 who was 37? (1)
d) si FOG=2, RAIN=5 et WIND=6, qu'est-ce que c'etait 12? (1)

(U) 33. If A + B = G; and T/I = L; and B x S = U; and L - K = I; and A + G = D; and K x K = U; and D! = A + G + K; what is the square root of R? (1)

(U) 34. Interpret the following:

1 5 7 8 9 10 12 13 14 17 18 19 22 26 29 33 35 39 43 48 49
1 2 4 5 7 12 15 17 20 23 25 29 33 35 36 38 39 42 44 47 50
1 3 5 7 12 15 17 20 24 30 32 35 37 39 41 45 47
1 5 7 8 9 12 13 14 17 18 19 24 31 35 39 41 42 43 44 45 48 49
1 5 7 12 13 17 18 24 30 32 35 39 41 45 50
1 5 7 12 14 17 19 24 29 33 35 39 41 45 47 50
1 5 7 8 9 10 12 15 17 20 24 29 33 35 39 41 45 48 49 (1)

7B. (U/~~FOUO~~) Solution to Previous Puzzle: "Disemvoweled," by [redacted]

(U) Each of the following is a group of related words. Each group has had its vowels removed (ouch!). For purposes of this puzzle, Y is always a consonant. The number in brackets indicates the number of words in the group. For each group, fill in the missing vowels, and identify the common feature.

[6] B S L R G N D L L C R N D E C M N M C
basil, oregano, dill, coriander, cumin, mace (spices)

[4] C N N M L R N C S R B C S P D

[redacted] (b)(3)-P.L. 86-36

[redacted]

canine, molar, incisor, bicuspid (teeth)

[6] K R C H N R S S L S N P L N D
Korea, China, Russia, Laos, Nepal, India (Asian countries)

[5] R L S M T S N G L S P D R S X P S
Orioles, Mets, Angels, Padres, Expos (Major League Baseball teams)

[6] R S D S Y R S P T N B G N D H L
iris, daisy, rose, petunia, begonia, dahlia (flowers)

[6] P L J V B S C C C B L D
APL (or PL/I), Java, BASIC, C, Cobol, Ada (programming languages)

[6] B V L T B C L L F L T P N
oboe, viola, tuba, cello, flute, piano (musical instruments)

[6] W H T W H T C H P T P T N N R Y
white, wheat, chapati, pita, naan, rye (breads)

[5] M R M G R T T D L M S S N R N S T
Miro, Magritte, Dali, Masson, Ernst (surrealist artists)

[6] B L S K T Y D D M T H B T L N T
bee, louse, katydid, moth, beetle, ant (insects)

[5] L S T N M N N W R Z N T T N C B N T Y
Lusitania, Minnow, Arizona, Titanic, Bounty (ill-fated ships)

[6] M R M N N Q N S H R D Y W L F P N
More, Mann, Aquinas, Hardy, Wolfe, Paine (writers named Thomas)

[6] T M T P F F F F N R D R C K M D S M G
Tiamat, Puff, Fafnir, Draco, Komodo, Smaug (dragons)

(U//~~FOUO~~) In the opinion of the Puzzle Czar, the best solution came from [redacted] whose solution agreed with the given one, except for the forgivable transgression of identifying the surrealists as merely modernists. Honorable mentions go to [redacted]

(U) Some solutions were, shall we say, creative. Here are some random comments from the czar on various attempts.

[dragons] I've never seen the magazines "Tipoff", "Affine", or "Roderick"...

[surrealists] Miriam, Gretta and Delma? Are they Borgnines or Hemingways?

[breads] "Naan" is a much better solution than "onion"; the latter stinks.

(b)(3)-P.L. 86-36

"""
//

8.(U) LETTER FROM THE EDITORS

(U//~~FOUO~~) We would like to take this opportunity to thank everyone who contributed articles and/or their time and effort to the _Tales of the KRYPT_ during 1999. Aside from those whose names appeared in this newsletter with their articles, and those listed on the Editorial Board below, we would like to recognize [redacted] who have often provided us with information we think has been important to publish to the CA Community.

(U//~~FOUO~~) We also thank [redacted], our outgoing President, for all your many hours that you devoted to the KRYPTOS Society. And special thanks to [redacted], our outgoing President-Elect, [redacted], outgoing Treasurer, and [redacted], outgoing Members-at-Large. Our organization is the better because of your service.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Congratulations to the many who retired after working so tirelessly, faithfully and effectively in the CA community. Among those to be saluted are: [redacted] (If you know of anyone we've overlooked, please send us a "Letter to the Editor" and we'll try to publish the name(s) in a future issue.)

(U//~~FOUO~~) We look forward to a brand new year (and completely new century numbers), and invite you to help us provide appropriate and useful information in the upcoming issues of the KRYPTOS Society Newsletter.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) [redacted]
Editors, _Tales of the KRYPT_

"""
//

9.(U) EDITORIAL CORNER

REMINDER: (U) Submissions for the next issue are due by 23 January, 2000.

(b)(3)-P.L. 86-36

[redacted]

PLEASE NOTE: (U) All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION-MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the editorial board.

(U//FOUO) Tales of the KRYPT Editorial Board
Editor:
Assistant Editor:
Puzzle Editors:

(b)(3)-P.L. 86-36

\\\

(b) (3)-P.L. 86-36

CONFIDENTIAL

(U) POC: [redacted] /nfo
(U) *Last Modified: 10/30/2002 11:42:25*
(U)PE EXTERNAL PAGE

~~FOR OFFICIAL USE ONLY~~

****
* TALES OF THE KRYPT *
****
January - February 2000

//
****
(U) TABLE OF CONTENTS:

1. (U//FOUO) PERSPECTIVE: "Musings of a Former Cryptologic Mathematician Program (CMP) Executive
by [redacted] Former CMP Executive

2. (U) CALENDAR OF EVENTS

3. (U//FOUO) CRYPTANALYSIS CAREER PANEL (CACP) NEWS
by [redacted] Assistant Executive, Cryptanalysis Career Panel

3a. (U) We've Moved!

3b. (U) Welcome Interns!

3c. (U) Wanted: Enthusiastic, Experienced Cryptanalysts

3d. (U) Registration for the 61st Cryptanalysis Professional Qualification Examination

4. (U) KRYPTOS SOCIETY NEWS

4a. (U//FOUO) KRYPTOS Society - A New (Unfortunately Slightly Lower) Profile
by [redacted] President, KRYPTOS Society

4b. (U) KRYPTOS Society Membership Drive

4c. (U) Breakfast Affair for Newly Certified Cryptanalysts (BANCC): Postponed But Not Forgotten

5. (U) COMMUNITY NEWS

5a. (U) MathFest 2000

5b. (U//FOUO) Center for Cryptologic History Talk: "The Dark Ages of American Cryptology", by Tom Johnson

5c. (U//FOUO) 1999 Cryptologic Literature Award Memorandum
POC for Message: [redacted]

5d. (U) Eighth Annual Signals Analysis and Development Conference

6. (U//FOUO) KRYPTOS PUZZLES (by [redacted]

6a. (U) New Puzzle: WANT MATH FLEET? FLATTEN WET HAM!

6b. (U) Solution to KRYPTOS KRISTMAS KWIZ

7. (U) EDITORIAL CORNER

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

****
//

1. (U) PERSPECTIVE: Musings of a Former Cryptologic Mathematician Program (CMP) Executive

by [redacted] Former CMP Executive

(U//FOUO) In August 1975 I arrived at NSA with a newly minted Ph.D, ready to start doing something I wasn't sure about. One thing stands out in my mind that first day: a Marine guard giving my car a waist-level salute as I drove in. I thought I was pretty hot stuff! (Now it may be that I did not receive a "real" salute, but rather some sort of waving in of my car. I do not want to know. I still get a self-satisfied feeling thinking about being saluted on my first day at work.)

(U//FOUO) After a blurred day or two of briefings, I reported to R51 (one of the few "fixed points" in the many reorganizations that I've seen), and shortly thereafter came my first visit to the CMP office. We were more formally known as the "P1 Cryptologic Mathematician Program" and informally as "P1" or "The P1 Program." The Chief of P1 was MISTER Lutwinjak, crossword puzzle writer for the New York Times. The CMP Exec was [redacted] recently returned from GCHQ, and the real power in the office was [redacted] was not a mathematician, but she seemed to have an innate understanding of what offices were doing which problems and who would fit in where. The standard operating procedure for new tours was very simple: [redacted] called you up and told you where you were going in two weeks. With a little whining you could delay or defer a tour, but not for long. [redacted] knew what was best!

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

(U//FOUO) Tour choices were simpler then; there just weren't as many offices for mathematicians to visit. The standard list of tours included R51 (still the same designator), [redacted] occasional tours available in "exotic" areas like satellites, speech, or engineering. The bulk of the work of a P1'er then was against [redacted]

(U//FOUO) It never occurred to me that 21 years later I would return to the CMP as its Executive. The two biggest changes that I have observed are 1) the large number of areas in which CMP'ers now tour and 2) the pervasive use of computers. We used computers a lot in the "old days," but not like today. I remember "tube rooms" where you'd sign up for hour blocks of time on a terminal. These rooms were darkened except for the flickering bluish glow from the CRT's. Because of the wait for tube time, you were often forced to be clever before you could even play with an idea on a computer. Times have changed!

(U//FOUO) Mathematics is recognized today as an essential tool for solving general problems, not just cryptanalytic problems. CMP'ers work with engineers, computer scientists, linguists, signals analysts, and others to solve some of our hardest problems. Many new CMP'ers are like kids in a candy shop as they contemplate the array of exciting problems they can work on.

(U//FOUO) Computers are ubiquitous now; it's hard to imagine an office without a workstation for everyone. When asked by applicants what they should study before starting work here, my stock answer is, "C and Unix." The area of Computer Network Analysis simply didn't exist 25 years ago, and it's fun to think about what new work areas will be created during the next 25 years.

(U//FOUO) [redacted] Within a week or so the Applied Math Program was born, and the NSA math community once again showed its ability to rise above bureaucracy and continue solving problems.

(U//FOUO) The future is secure for clever problem solvers at NSA. I can't tell you what tools will be needed next year, nor can I tell you what the hot problems will be, but I am certain there will always be a place for technological innovators. And I hope that CMP graduates will continue to take the lead in problem solving innovations.

(U//FOUO) The one thing I've been mulling over is if there's a CMP'er who EOD'ed during my tenure who'll become CMP Exec in 20 years. I guess I'll have to wait and see, and hope they'll consider inviting a "has-been" to the graduations and picnics.

(b)(3)-P.L. 86-36

---

2. (U) CALENDAR OF EVENTS

Mar 24	(U) Deadline for Abstracts for MathFest 2000 (See article 5a.)
Mar 24	(U) Deadline for 2000 KRYPTOS Membership Drive (See article 4b.)
Mar 29	(U//FOUO) Center for Cryptologic History Talk Tom Johnson; 0930 in HQ, room 9A135 (See article 5b.)

(U) PLAN AHEAD

Apr 17	(U) Deadline for 1999 Cryptologic Literature Award Entries (See article 5c.)
May 9-10	(U) 61st Cryptanalysis Professional Qualification Examination (CA PQE) (See article 3d.)
May 22-26	(U) Eighth Annual Signals Analysis and Development Conference (SADC) at NSA, Ft. Meade (See article 5d.)
Jun 9	(U) MathFest 2000 R & E Symposium Center on Friday 0830-1630 (See article 5a.)
Jun 19	(U) Breakfast Affair for Newly Certified Cryptanalysts (See article 4c.)
Jul 31	(U) KRYPTOS Society Literature Contest Deadline

(b)(3)-P.L. 86-36

[redacted]

3. (U//FOUO) CRYPTANALYSIS CAREER PANEL (CACP) NEWS
by [redacted], Assistant Executive, Cryptanalysis Career Panel

(b)(3)-P.L. 86-36

3a. (U) We've Moved!

(U//FOUO) We've moved! The Cryptanalysis Career Panel Home Page has moved. In addition, we are updating information, adding new pages, and refurbishing the old ones. If you cannot find what you are looking for or have suggestions for the pages, please contact the CACP office at h111@nsa or [redacted] Please update your bookmarks:

[redacted]

3b. (U) Welcome Interns!

(b)(3)-P.L. 86-36

(U//FOUO) The CA Intern Panel welcomes its newest interns:

[redacted] hired in January;

[redacted] hired in February; and

[redacted] hired in March.

(b)(6)

3c. (U) Wanted: Enthusiastic, Experienced Cryptanalysts

(U//FOUO) The Cryptanalysis Career Panel desires to match enthusiastic, experienced cryptanalysts with CA interns and cross-trainees for career development and technical guidance throughout their programs. This will provide additional technical advice to the participants as they learn the skills, knowledge, and tools of Cryptanalysis--and how much fun it can be!

(U//FOUO) If you are interested in serving as an advisor to an intern or cross-trainee, please provide the following information to h111@nsa:

Name: Sid:
Organization: Phone:
Your areas of interest/expertise:

3d. (U) Registration for the 61st Cryptanalysis Professional Qualification Examination

(U//FOUO) Registration for the 61st Cryptanalysis Professional Qualification Examination (CA PQE) will be held from 6 March through 14 April for eligible aspirants. Early registration is encouraged so that all pretest requirements can be validated. The 2000 CA PQE will be given on Tuesday and Wednesday, 9-10 May 2000, at the FANX2 complex. Registered, eligible aspirants should report both days at the time and location listed below:

Building	Room	Report Time	Exam Begins	Exam Ends
FANX II	A2B020 or A2B024	0815	0830	1230

A Privacy Act Statement will be signed the first day of the test for use of social security numbers in releasing scores.

[redacted]

(b)(3)-P.L. 86-36

(U//FOUO) Eligibility: each aspirant must verify his/her eligibility for the CA PQE with the CA Career Panel office--H111, OPS2B Room 3036D, [redacted] Aspirants who have previously taken the CA PQE are eligible for the 2000 CA PQE; those who have not taken the CA PQE must successfully complete/have credit for CA107, CA110, and CA123; one year of cryptanalytic experience, and two diversity assignments. For new aspirants, H111 must also receive a copy of their Diversity Tour Validation Sheet to verify two diversity assignments and their latest Personnel Summary (PERSUM) for cryptanalytic experience by 14 April 2000.

(U//FOUO) PQE review sessions will be held every day during the month of April, during lunch hours, so as not to interfere inordinately with office work time. It is strongly suggested that aspirants prepare for these sessions by working the questions from the previous examinations. Aspirants should come to the review sessions with specific questions or examples to share. Since some of the review sessions will be held in small conference rooms, only those people taking the exam will be allowed to attend. Copies of the schedule will be available from [redacted]

(U//FOUO) Independent review sessions are being held currently.

(b)(3)-P.L. 86-36

[redacted]

Contact [redacted] for more details; or see [redacted] CA PQE Review Session Web Page for information.

(U//FOUO) Please direct any questions to the CA Career Panel Office, hl11@nsa, [redacted]

---

4. (U) KRYPTOS SOCIETY NEWS (b)(3)-P.L. 86-36

4a. (U//FOUO) KRYPTOS Society - A New (Unfortunately Slightly Lower) Profile
by [redacted], President, KRYPTOS Society

(U//FOUO) On 2 February, [redacted] as the new President of the KRYPTOS Society, attended a meeting called by the Council of Learned Organizations. [redacted] from the ethics office, was the guest speaker. The bottom line of her comments was that, from an ethics point of view, organizations are either non-federal or federal; there is nothing in between. Virtually all of NSA's Learned Organizations (LO's), including KRYPTOS, were created as non-federal entities. Consequently, they can function outside of many of the rules that apply to the Federal Government, particularly the rule about conducting business as Congress indicates and only with appropriated funds. LO's have their own funding and can use it as they please. On the other hand, members cannot use Agency time, supplies, or other government resources in support of the LO's day-to-day operations. Government employees may contribute to KRYPTOS (or any Learned Organization) by writing papers, preparing talks, or attending functions (assuming these activities are related to their jobs) on official time, but they cannot organize any of those events during work hours. A limited use of e-mail is allowed. E-mail may be sent on behalf of a Learned Organization to their members, but not to a mass distribution. LO's can (and should) have WEB sites and ESS topics to convey information to others in the community. The saving grace is that NSA LO's can partner with other federal organizations to advertise their activities. KRYPTOS will work with the Cryptanalysis Career Panel and with ? Group in efforts that continue to support our cryptanalytic workforce. One problem that cannot easily be solved is our ability (or inability) to conduct membership drives. Please keep an eye on the KRYPTOS website [redacted] for details of this and other issues. The KRYPTOS Council will do its best to keep the Cryptanalysis Community informed while staying within the legal guidelines that we have been given. (b)(3)-P.L. 86-36

(U//FOUO) In a related matter, the Editor of _Tales of the KRYPT_, the KRYPTOS Society Newsletter, responded to a new Agency directive on publication review by providing information on the purpose, scope, audience, resources used, and process of producing the newsletter. The Office of Corporate Communications recently notified the editorial staff that the _Tales_ is approved to continue publication during 2000; and subject to an annual review, in the future.

4b. (U//FOUO) KRYPTOS Society Membership Drive (b)(3)-P.L. 86-36
by [redacted]

(U//FOUO) The 2000 KRYPTOS membership drive is on! The KRYPTOS Society was established in 1981 to promote interest in cryptanalysis, to provide a focal point for the fields of common interest to cryptanalysts of the National Security Agency, and to promote excellence in the cryptologic community.

(U//FOUO) If you are interested in cryptanalysis and like to see technical excellence encouraged and rewarded, please consider supporting the cryptanalytic community by joining KRYPTOS!

(U//FOUO) To join, please pay the dues ($5) to one of the following people and fill out a short form: (b)(3)-P.L. 86-36

[redacted]

(U) Of the people who have joined by March 24th, 10 lucky people will receive $10 gift certificates to Border's Bookstore!

(U//FOUO) If you prefer, please fill out the following and mail along with $5 to [redacted] OPS2B 2B4012: (b)(3)-P.L. 86-36

Name:
Room Number:
E-mail Address:
Interested in chairing a committee? ____ Yes ____ No
Interested in working on a committee? ____ Yes ____ No
If "Yes", please check committees of interest to you:
___ Where needed
___ Awards

(b)(3)-P.L. 86-36

[redacted]

___ Cryptanalytic Literature
___ Distinguished Members
___ Membership
___ Program
___ Publicity
___ Retired Members
--- Newsletter

(FOUO once filled in)

4c. (U) Breakfast Affair for Newly Certified Cryptanalysts (BANCC): Postponed But Not Forgotten

(U) Mark your calendars for the Sixth Annual BANCC Breakfast Affair For Newly Certified Cryptanalysts

Sponsored by KRYPTOS

Monday, June 19, 2000
8:00 to 10:00 a.m.

Stay on the lookout for more details of this popular event. Tickets will go on sale in May!

(U//FOUO) Those of you who pay attention to the social activities in the CA community may have noticed that you have not yet seen an announcement for the annual BANCC (Breakfast Affair for Newly Certified Cryptanalysts) which is jointly sponsored by the Cryptanalysis Career Panel and the KRYPTOS Society, and is usually held in February. It has been postponed until June 19. This was done for several reasons. Since there have been so few people hired into the CA career field over the last few years, the number of newly certified cryppies has been low (and is very small at this time). We hope that by June, there will be more who are certified. Secondly, it's always a bit unnerving to plan a social activity in a month where the weather is unpredictable. We feel pretty confident that we won't get snowed out in June, so start now in working up an appetite and we hope to see you all on June 19!

****
//////////

5. (U) COMMUNITY NEWS

5a. (U) MathFest 2000

(U) This is a call for ABSTRACTS for MathFest 2000.

(U//FOUO) MathFest is a day-long festival presented by the Cryptomathematics Institute to showcase the highlights of the past year in cryptomathematics. Its purpose is to bring NSA cryptomathematicians (and all other interested, cleared parties) together for a day to celebrate the unique and varied contributions that our discipline makes to the success of the NSA mission and to emphasize the challenges and opportunities that the future holds for our community.

(U//FOUO) MathFest 2000 will be held in the R & E Symposium Center on Friday, June 9, 2000, from 8:30 am until 4:30 pm.

(U//FOUO) If you have a noteworthy accomplishment, significant work in progress or a survey of work that you would like to present, this is a golden opportunity to share it with your colleagues in the community. Talks will be from 20 to 30 minutes in duration and classification can be up to TS//SI//COMINT/[redacted]

(U) For determining the suitability of a topic the MathFest 2000 Committee has a very broad and inclusive definition of mathematics. We do ask, however, that presentations be understandable by a general math audience.

(U) The DEADLINE for abstracts is the close of business on Friday March 24, 2000. For the convenience of the committee, abstracts should be in 12 pt. type in one of the following soft formats:

a) Framemaker
b) PDF
c) Postscript

Further we ask that abstracts be no longer than one page in length.

(U//FOUO) Abstracts should be sent to the MathFest 2000 Committee Chairman, [redacted]

(U//FOUO) The MathFest 2000 Committee is:

[redacted] also [redacted]

(U) Any one of us will be happy to answer any MathFest questions you may have.

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

5b. (U//FOUO) Center for Cryptologic History Talk: "The Dark Ages of American Cryptology", by Tom Johnson

(U) The organization is floundering. It has lost its sense of purpose--former enemies are friends, and no one knows who the new enemies are. Its best people are leaving, or have already left, for the higher pay and better conditions of private industry, or to the comfortable existence of college faculties, or to an honorable retirement. It has fallen behind technologically. The best computer wonks work for Beltway Bandits, and it lacks money to buy the latest machines and software. It is being attacked from all sides by organizations anxious to divide the spoils and run off with the mission. Like vultures, they wait for the inevitable demise.

(U) Y2K? No, 1952. Guess what? We've been through this before. NSA, created in 1952, was almost killed in its cradle. What did the organization do to survive? How did it fend off the wolves? What solutions did it devise?

(U//FOUO) Tom Johnson, formerly with the Center for Cryptologic History, will discuss the problems of 1952 and how the Agency survived. There might even be some lessons there.

(U) You can hear Mr. Johnson's talk, sponsored by the Center for Cryptologic History, on Wednesday, 29 March, at 0930 in HQ, room 9A135.

5c. (U//FOUO) 1999 Cryptologic Literature Award Memorandum (b)(3)-P.L. 86-36
POC for Message: [redacted]

1. (U) All NSA and SCE personnel who have written and published a paper, monograph, study, history, or article during 1999 which meets the criteria in paragraph 2 of this memorandum, are invited to submit their papers for the CY1999 Cryptologic Literature Award. This award was established in 1962 by VADM L.H. Frost, USN, Director, NSA, as the highest award to recognize contributions to cryptologic literature. To ensure that no contribution which merits consideration is missed, I encourage all Agency officials and SCE commanders to bring noteworthy contributions to the attention of the Cryptologic Literature Review Board.

2. (U) The criteria used by the Board to review and recognize noteworthy contributions are:

a. (U) Relevance: The writing must have a direct and significant connection with cryptology and be of substantial cryptologic importance.

b. (U) Validity: The writing should be solid in its premise and sound in its reasoning.

c. (U) Craftsmanship & Style: The papers should be written in easily understood English and have broad intellectual appeal to the entire cryptologic community. They should not be so specific in content that they are understood and appreciated only by experts in cryptologic disciplines. Papers should follow generally accepted guidelines for grammar, style, spelling, and organization.

d. (U) Originality: The writing must be original or cover new facets of a given subject.

3. (U) Awards of $2,000 for first place, $1,200 for second place, and $800 for third place will be presented by the Chief, Global Learning Services, S3, at a formal ceremony.

4. (U//FOUO) Authors should send two copies of their papers with a cover sheet to the Executive Secretary of the Review Board, [redacted] by 17 April, 2000. If you have any questions regarding this award, please contact [redacted] or by e-mail as [redacted] For more information and a copy of the necessary cover sheet visit us on the web: [redacted] (b)(3)-P.L. 86-36

5d. (U) Eighth Annual Signals Analysis and Development Conference

(U//FOUO) Z6 is pleased to announce the dates for the Eighth Annual Signals Analysis and Development Conference (SADC). This conference is sponsored by Z6, [redacted] The dates for the conference are 22-26 May, 2000 at NSA, Ft. Meade. This conference will provide an exchange of technology and signals analysis work through a series of briefings, open discussions, and working groups.

(U//FOUO) The theme for this year's SADC is "Signals Analysis: The Foundation for Exploiting Tomorrow's Technologies." This conference provides the opportunity to share knowledge, experience, and ideas with colleagues. We hope that this will be a "two-way street" and that you will gain as much as you give. The only way that this will be a success is if you take an active involvement in the conference. Take advantage of this opportunity to give knowledge by presenting a topic and to gain knowledge by attending the conference.

(b)(3)-P.L. 86-36

[redacted]

(U//~~FOUO~~) Although it is not necessary at this time, you may submit abstracts of what you would like to present. Additionally, we welcome any ideas for topics that you would like to see. We will make every effort to find a presenter for the suggested subject matter. All proposed presentations will be reviewed by the SADC Leadership team. If possible, please prepare presentations in Powerpoint format. Site overviews are discouraged (except for the ones being coordinated separately for the field position presentations).

(U//~~FOUO~~) As usual, the conference will offer opportunities to meet others in the signals analysis field, as well as become familiar with the faces of people you have corresponded with from around the globe.

(U) The following activities are being planned:

Breakfast on Monday morning
Signals Analysis information on field positions
Two-day vendor expo
Conference social on Thursday night

(U) Another message will be sent out shortly with more specifics including dates that the abstracts are due and prices for the social activities. We wanted to allow as much time to schedule the conference into your plans and for you to formulate ideas on briefing subjects.

(U//~~FOUO~~) Please forward the names of proposed attendees, e-mail addresses, and secure phone numbers. Include any ideas. If you are planning on preparing a presentation, please include a title, a short abstract, the highest classification (not to exceed TOP SECRET COMINT), time required, and any equipment required.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) [redacted] is our Chair for SADC 2000. Responses and questions may be directed via e-mail to [redacted] or call [redacted]

(U) Visit our web site at:

[redacted]

//

6. (U//~~FOUO~~) KRYPTOS PUZZLES (by KRYPTOS Puzzle Editors: [redacted]

6a. (U) New Puzzle: WANT MATH FLEET? FLATTEN WET HAM!

(U) The puzzle editor who was scheduled to contribute this issue's puzzle was conveniently TDY at the time the puzzle came due. The other two puzzle editors would never stoop to embarrassing the missing party by naming names, so they have valiantly stepped in with some crypto-math to save the day. You know what to do.

(U//~~FOUO~~)

[redacted]

```
      N T M L E              * * *
    F A M M H              * * * * *
    M A T T              * * * * *
  N M H C L            * * * * *
  R H E A            * * * * *
  --------------     ---------------     ---------------
  L A C E R A T E    B R E A K F A S T   C O G I T A T E
```

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Please send solutions to this puzzle to [redacted]
Please send new puzzle ideas to [redacted] or [redacted]

6b. (U) Solution to KRYPTOS KRISTMAS KWIZ

(U//~~FOUO~~) We were pleased with the number of people who took the time to enter the 1999 KRYPTOS Kristmas Kwiz. The winners, with a very impressive score of 98.5, are the team of [redacted] Each of the winners will receive a KRYPTOS Society mug. [redacted]

(b)(3)-P.L. 86-36

(b)(6)

(U//~~FOUO~~) The other teams who entered also did very well. Those teams include: [redacted]

(U) The short version of the answers appear below. More complete answers, with some additional explanations can be found on the KRYPTOS website [redacted] If you haven't had much luck in the past with the Kwiz, look there for explanations that will hopefully help you in Kwiz's to come. And now, on to the answers!

(U) 1. The most common answers are ewe & you, I & aye, and I & eye.

(U) 2. The word PONY goes between STRESS and RIFF. There are 5 groups of ten elements each which fit into the groups: letters of the alphabet, creepy-crawlies, Christian names, jobs, and x's y (i.e.

(b)(3)-P.L. 86-36

[redacted]

Plank's CONSTANT).

(U). 3. ERRORS: This question had two problems in the original form. The numbers 1 and 1875 were swapped and the fourth value (44) should be a 4.

(U) The number 55 goes in the list between 1 and 1752. We have 7 groups with 8 elements in each group. The groups are: animals associated with Chinese years, numbers between 1 and 8 in German, prefixes associated with powers of 10, gifts for days 1 through 8 of Christmas, country's dates for Julian to Gregorian calendar conversion, wedding anniversary gifts, and atomic numbers of elements associated with heavenly bodies.

(U) 4a. SCOWL. The others make animals from their outer letters. SCOWL makes it from its inner letters.

4b. BAIT. The others form words with BLACK. BAIT is associated with WHITE.

4c. TROUBLES. All the other words alternate letters between parity groups. TROUBLES switches groups every two letters.

4d. IDEA. All the other words are Arabic in origin.

4e. IDEA. The others have synonyms which end in "ORT".

(U) 5. The answers form a word square.

M O S E S
O F T E N
S T A R E
E E R I E
S N E E R

(U) 6. The longest sentence had 59 consecutive 2 letter words, and most were pretty contrived, but we gave them credit anyway.

(U) 7. The theme is numbers in the native language whose letters are in alphabetical order.

(U) 8a. Good Answers: PARING, PROPER, BOATER, DESERT, PARLEY, CURING. Word n of the sequence can have the letter in position n of KRYPTOS added in the middle of the word to form another word.

8b. Good Answers: JEEP (becomes KEEP), JILT (becomes KILT). Word n in this sequence can have the nth letter of the alphabet replaced with the (n+1)st letter and still form a word.

8c. Good Answers: UNFED, FUNNEL, FUNHOUSE, FUNERAL, CONFUSE. Word n contains all the letters from the French word for n.

8d. Good Answers: RIVER (to ARENA), ERG (to NAP), SIRE (to BRAN). For word n, changing each letter to one n later (cyclicly) also forms a word.

8e. Good Answers: (ide)A, (ide)ALLY, (impala)TABLE, (ibis)OR. Animals starting with consecutive letters can be added before or after the word in an alternating manner and still get a word.

8f. Good Answers: PIGlet, WAYlay, EYElid, BOWled, PALlid, GALlop. Words can be followed by words starting with consecutive letters.

8g. Good Answer: JONQUIL. Alternating 6 and 7 letter words with the first letter moving from A, B, C,... and the 4th letter going from Z, Y, X,...

8h. Good Answers: RHYME, HOUR, HERBAL, CHORD, LIGHT, HONOR. Word n has a silent letter which is the nth letter of the alphabet.

8i. Good Answers: VICIOUSNESS, VICEROYALTY. Using A=0, B=1,..., Z=25, the first letters of each word form a Fibonacci sequence. Also, the sum of all the letters gives another Fibonacci sequence.

8j. Good Answers: MAZE, AMAZE, AMAZING. Word n contains the nth and (n+13)th letter of the alphabet.

8k. Good Answers: ACCOUNTANT, DEPARTMENT. Word n has the first letters of numbers n and n+1 in positions n and n+1 of the word and has no other positions where that property holds.

8l. Good Answers: INCONVENIENCE, INTERDEPENDENCE. Word n has n letters in common with the spelling of the number n.

(U) 9. The best word found is 11 letters long, AUSTRINGERS.

(U) 10a. HG Wells
b. GK Chesterton
c. HE Bates
d. AE Housman
e. PG Wodehouse
f. CS Forrester
g. CP Snow
Using the appropriate letters, we get the name WH Auden. Answer using a cryptic clue like "Wed a Hun? Frightful!"

(U) 11. The best words found for each size were as follows:

a. adoperated - ado, dop, ope, per, era, rat, ate, ted
b. propends - prop, rope, open, pend, ends
c. traverses - trave, raver, avers, verse, erses

(U) 12a. The first column is the list given in the problem. To get the second column, we anagram the first list. The third list is found by phrases of the form x AND y. For example, CATS and DOGS. Then the last column is an anagram of the third column into alphabetical order.

GODS	DOGS	CATS	ACTS (or CAST)
VASE	SAVE	SCRIMP	CRIMPS
GROWN	WRONG	RIGHT	GIRTH
STAPLER	PLASTER	LATH	HALT
EARTHY	HEARTY	HALE	HEAL
DIET	TIDE	TIME	MITE (or ITEM)
CANED	DANCE	SONG	NOGS
SERVE	VERSE	CHAPTER	PATCHER
SADDLER	LADDERS	SNAKES	SNEAKS (or SKEANS)
SNAP	PANS	POTS	STOP (or SPOT)
BLOTS	BOLTS	NUTS	STUN
PLACER	PARCEL	PART	TARP (or TRAP)
PRIESTS	STRIPES	STARS	TRASS (or TSARS)

12b. The first column is the original list. To get the second word, we use a foreign synonym. Then the third column is the country of origin of the words in the second column. Finally, the fourth column is the capital of the third column.

BIRDWATCHER	ORNITHOLOGIST	GREECE	ATHENS
BOMBING	BLITZ	GERMANY	BERLIN
BEEF STEW	GOULASH	HUNGARY	BUDAPEST
DAGGER	KRIS	MALAYSIA	KUALA LUMPUR
BROAD-BRIMMED HAT	SOMBRERO	SPAIN	MADRID
OPENNESS	GLASTNOST	RUSSIA	MOSCOW
DEAD END	CUL-DE-SAC	FRANCE	PARIS
OPEN PIE	PIZZA	ITALY	ROME
GRIEVANCE OFFICIAL	OMBUDSMAN	SWEEDEN	STOCKHOLM
DRUMBEAT	TATTOO	HOLLAND /	THE HAGUE
PAPER-FOLDING	ORIGAMI	JAPAN	TOKYO

Other possibilities are:
for SOMBRERO, the country is MEXICO and the capital is MEXICO CITY;
using TABOR instead of TATTOO gives IRAN with the capital TEHERAN;
using DIRK instead of KRIS and gives SCOTLAND and EDINBURGH;
using SKENE instead of KRIS gives IRELAND and DUBLIN.

(U) 13. 3637 or 3435. The digits stand for the number of letters in each word of the country's national anthem. The national anthem for New Zealand is "God Defend New Zealand" or "God Save The Queen."

(U) 14. Taking the first letter of each number's spelling gives a word for all the sequences except (4 12 7 15 9 8).

(U) 15. The three best solutions we received were the following:
Sqrt(Sqrt[97 + ((.81)recurring / Sqrt(4)) + (2^(-6) * 50^(-3))]] which gives a value of 3.14159265359051 which differs from pi by 7.133 x 10^-13

Sqrt((2143/(98-76))^0.5) which gives a difference of 1.00715x10^-9

3.841(5926) - 0.7 with a recurrence over the 5926. This gives a difference of 5.67613x10^-9.

(U) 16a. The first n digits of the number are divisible by n.

16b. The digits are in alphabetical order.

(U) 17. 22 17 17
-1 66 5
19 6 22

(U) Row 1 is cyclicly shifted 1 place right each step. The values are obtained by adding 2, finding the next prime, and adding 1 from one step to the next. The concatination of positions 2,3 and 3,2 are found by adding 7 from one matrix to the next. The value in position 3,1 is the value of the corresponding letter of KRYPTOS. The value in position 3,3 is 5 plus the value in position 1,2. The sum of the first column is 40, so we can solve to get position 2,1. Finally, the center block is obtained by the absolute value of the product of the differences of the other two values in the same row and the same column. Here that is (17-6)*(5-(-1)) = 66.

(U) 18a. All the trigraphs here appear in the question for #18.

18b. All are the beginnings of Capital cities.

18c. All have the letters in alphabetical order.

18d. All are the beginnings of composers names.

18e. International Vehicle Registrations

18f. All are words backwards.

18g. All form words when each letter is replaced with the next letter in the alphabet.

18h. All words appear twice in previous lists.

(U) 19a. All the words before the colon have sum of letters equalling 70. ABSENTEE has a word sum of 71.

19b. The words before the colon have letters from KRYPTOS SOCIETY.

19c. Each word before the colon has 5 consecutive letters in some order.

19d. Words before the colon can be typed using only the letters on the top row of the keyboard.

19e. The letters in the alphabet are broken up into three groups depending on their value mod 3. The words before the colon come solely within one of those three groups of letters.

(U) 20a. All are place names when capitalized and pronounced differently.

20b. All died in a year which is a perfect square.

20c. Change one letter in each to get a US President.

20d. All become words when digits are replaced with Roman numerals.

20e. All become plural when 1 S is added and singular again with a second S.

20f. All become words when expressed in hexadecimal.

20g. All are anagrams of composers.

(U) 21. By looking at the first letter of each word in this list (left to right from top to bottom) we see PERFORM FREQUENCY COUNTS. Doing this, you should notice that there is no L. Thus, the name of the friend is NOEL.

(U) 22. Each element of the list was a country which had one letter changed and then anagrammed.

(U) 23. The best words we got were:
a. Blepharoconjunctivitis (win at V)
Neuropharmacologists (win at U)

b. Superacknowledgement (lose at V)
Dermatoglyphics (lose at U)

(U) 24. Thomson (Lord Kelvin). These people are related to temperature scales.

(U) 25. There are several word pairs that give all sixteen 4-letter words. CODE and MATS, TAPS and CONE, CAPE and TORS.

(U) 26. Each author has written a book (in one case a poem) with a title containing a character's first name but no last name. The first letters of these names form the question WHAT LINKS THEM? The answer is the first sentence of this answer.

(U) 27. The sum of the factors of each number (excluding the number itself) is equal to one of the other numbers in the group.

(U) 28a. 11 = Sides of a Hendecagon

28b. 12 = Dozens in a Gross

28c. 95 = Theses of Martin Luther

28d. 1936 = Forty Four Squared

(U) 29. .2 The equations are in duodecimal (base 12) arithmetic.

(U) 30. Group 1: The number corresponds to the largest number in the native language that contains the same number of letters as the number it represents. Using that, WALES gets a score of 3.

Group 2: The score is the number of colors in the country's flag. For ALBANIA, they get a score of 2.

Group 3: The score is the number of letters in the country's currency. For FINLAND, the score is 6.

Group 4: The smallest distance in the alphabet between two letters in a country's name. For LAOS, the score is 3.

Group 5: The number of hours the country's capital is ahead of Greenwich Mean Time. For HOLLAND, the score is 1.

Group 6: The score is found by taking the number of letters in the country name minus the number of letters in its capital. For SRI LANKA, the score is 1.

Group 7: The score is given by the number of answers with vertical symmetry. For AUSTRALIA, the score is 6.

Group 8: The score is given by the number of answers with horizontal symmetry. For UKRAINE, the score is 3.

(b)(3)-P.L. 86-36

9/24/2010

(U) 31. The pairing is as follows:

YELLOW + BIRD = YELLOWBIRD
INDIGO + CAST = DIAGNOSTIC
VIOLET + CAUP = COPULATIVE
BLUE + DOTS = DOUBLETS
ORANGE + FILM = LAGENIFORM
GREEN + PILL = REPELLING
RED + WITH = WRITHED

Notice that each of the words has no letters in common with the color that is associated with it.

(U) 32a. Based on US state nicknames and the order that they were admitted to the union. 40 is COYOTE (South Dakota is the 40th state).
ERROR: PELICAN should be associated with 18 not 9.

32b. 92 is U. They are the atomic numbers for each element.

32c. 37 is WILLIAM. He is England's 37th Monarch since 1066.

32d. 12 is FRUIT. The 12th month of the French Revolutionary Calendar was FRUCTIDOR.

(U) 33. I (or 10). The Greek letters also served as numbers.

(U) 34. By coloring in the appropriate squares in a 7x50 matrix, you get the phrase MERRY XMAS.

//

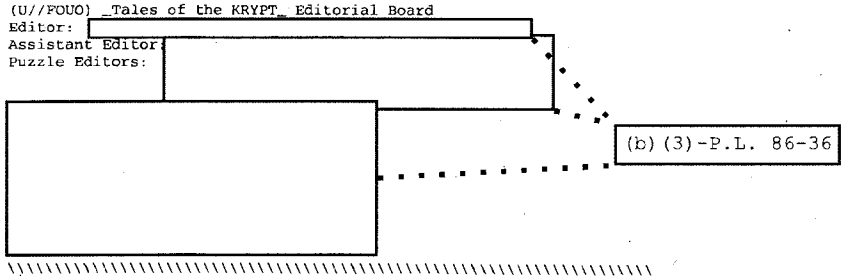
7.(U) EDITORIAL CORNER

REMINDER: (U) Submissions are welcome at any time, but in order to be published in the next regularly scheduled issue, are due by 6 April, 2000.

PLEASE NOTE: (U) All submissions must be in ASCII format, and, with the implementation of E.O. 12958, MUST BE PORTION-MARKED. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the editorial board.

(U//FOUO) _Tales of the KRYPT_ Editorial Board
Editor:
Assistant Editor:
Puzzle Editors:



\\\

~~FOR OFFICIAL USE ONLY~~

Derived from: NSA Classification Guide 342-98
3 August, 1998
Declassify on X1

~~CONFIDENTIAL~~

(b)(3)-P.L. 86-36

9/24/2010

(b) (3)-P.L. 86-36

~~CONFIDENTIAL~~

(U) POC: [redacted]
(U) *Last Modified: 10/30/2002 11:42:25*
(U)PE EXTERNAL PAGE

(UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~)

****
* TALES OF THE KRYPT *
****
Issue 1, 2001

****

(U) TABLE OF CONTENTS:

1. (U//~~FOUO~~) PERSPECTIVE: "In Defense of Loose Cannons"
by [redacted] Cryptanalyst

2. (U) CALENDAR OF EVENTS

3. (U//~~FOUO~~) CRYPTANALYSIS SKILL COMMUNITY PANEL NEWS
by [redacted] Assistant Executive, Cryptanalysis Skill Community Panel

3a. (U) Personnel Change

3b. (U) Welcome Interns!

4. (U) KRYPTOS SOCIETY NEWS

4a. (U) KRYPTOS Society Council Members, 2001

4b. (U) KRYPTOS Society 2001 Membership Drive

5. (U) COMMUNITY NEWS

5a. (U) SAWUNEH, 2001

5b. (U//~~FOUO~~) Upcoming CNE SCAMP

6. (U) FIGURES FROM THE PAST

6a. (U//~~FOUO~~) Reminder of a Colorful NSA Character,
by [redacted] President-elect, KRYPTOS Society

6b. (U//~~FOUO~~) Jacqueline Jenkins-Nye, World War II Code breaker
(Excerpts from a Baltimore Sun newspaper obituary, provided by [redacted] President-elect, KRYPTOS Society)

7. (U//~~FOUO~~) KRYPTOS PUZZLES
by [redacted] (b) (3)-P.L. 86-36

7a. (U) New Puzzle: "Jump-All-But-One Game"

7b. (U) Solution to "WANT MATH FLEET? FLATTEN WET HAM!"

7c. (U) 2000 KRYPTOS KRISTMAS KWIZ Winners

8. (U//~~FOUO~~) REAL WORLD CA CHALLENGE: HELP WITH A CODE?
(Request from the Center for Cryptologic History; by Barry D. Carleen, Chief, Publications Center for Cryptologic History)

9. (U) EDITORIAL CORNER

****
//

1. (U//~~FOUO~~) PERSPECTIVE: "In Defense of Loose Cannons"
by [redacted] Cryptanalyst, SID Planning

(U) Recently I overheard one employee describing another as a "loose cannon" and it was not intended as a compliment. In point of fact, all of us can name folks we would characterize as loose cannons. So what's the deal with loose cannons?

(U) NSA, like many mature bureauracies, places significant value on going along to get along. In management-speak this is called consensual management and its practioners--" team players". Those who are adept become respected and valued members of the community. Those who are not adept quickly become outliers and in extreme cases-- pariahs. [Okay, so this is an oversimplification but it's my problem ...]

(U) The good news is that consensual management with its emphasis on teaming is effective and provides tangible and significant benefits to the organization. Among these are: a stable working environment, a measured approach to decision making, and buy-in by the principal stakeholders. In other words it's good for business; almost everybody benefits.

(U) But there are some down sides and the bad news is that without sustained management attention our culture will produce some unwanted effects. Chief among these are: risk avoidance, diffusion of accountability, painfully slow and potentially unresponsive decision making, and my favorite--an erosion of the creative impulse. In other words, the opposites of the attributes which characterize

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

entrepreneurial enterprises.

(U) If you buy into this, then the issue becomes one of balance. It's how to avoid the anarchy of having large numbers of folks doing their own weird thing in order to gain and maintain a creative edge and how to realize the benefits of consensual management without sliding into mediocrity and the slow corporate death which is the end result of over reliance on consensual management.

(U) Not suprisingly, this is old news. And NSA's response has been ENPOWERMENT. Empowerment, if it actually occurs, is a partial solution. However, anybody who has decision-making authority is naturally reluctant to turn it over to a bunch of bananas. [If YOUR career/org/... were on the line you might be a bit controlling too!] Therefore, there are limits on the expectations of empowerment vis-a-vis ideation and change. Even with its built-in limitations, I saw little convincing evidence of actual empowerment until the arrival of the new guy at the top. No proposed action/initative was too small to not require sign-off by a seemingly endless chain of higher authorities. Form was often as important as content; a comma splice could spell the doom of an idea. Let's all hope that this has and stays changed. Smart enpowerment does not mean senior managers do not have a voice or vote, they simply choose more wisely where and when to weigh in. They delegate decision-making authority and hold ther delegatees personally responsible and accountable for the quality and effectiveness of their decision-making and this is repeated down the food chain. No rocket science here.

(U) Empowered or not, there will always be a need for fresh new ideas regarding who we are, what we do, how we do it, and how we market it. But as a class the poor old loose cannons are still not invited to the party. Should they be? Yes, if a way can be found to limit collateral damage.

(U) LC's fall into two broad categories;

1. Those who have uninformed opinions on everything and are not shy about sharing them, invited or not, in an inappropriate manner in all the wrong places. The typical Type 1 LC is cynical, negative, and organizationally destructive. You KNOW who I mean.

2. Those who, although marching to a very different tune, see and value that which 'works' in our business but do NOT feel personally bound to support that which in their view is not 'working or workable'. Unlike Type 1's, Type 2's do not actively oppose decisions once made. After being battered once or twice by managment for not not playing along, the usual response of Type 2 LC's is to tune-in and drop out. They become invisible and completely work-centric.

(U) Organizations and managers deal with ALL LC's the same way, isolation and ridicule. And once tagged and isolated, we ensure that it is a class four containment. Escape (or input) is impossible. Maybe there is a better way, (at least for the Type 2s).

(U) I know what I think and I am pretty sure of what my homogeneous colleagues think. If I need a different slant/insight on a problem/issue/process I am far more likely to obtain it from one or more LCs than from any other segment of our population. Of course, a good fraction (most?) of these 'views' will be from the planet Orkono and unworkable in this galaxy.

(U) But once in a while, just often enough to justify the aggravation, the view from the fringe will be new, exciting, useful, and workable!

(U) So folks, treasure and engage your "different" for among them may be the author of the idea that changes our world. Besides, it will make me feel more appreciated.

****
//

2. (U) CALENDAR OF EVENTS

Apr 12-Jun 29 (U//FOUO) SAWUNEH; CSE
(See article 5a.)

(U) PLAN AHEAD

May 7 (U//~~FOUO~~) KRYPTOS Society Talk: "The Algorithmic Mind of Bill Hayden," 1300-1530; (seating begins at 1315) Friedman Auditorium

Jun 11-15 (U) 2001 Signals Analysis and Development Conference (SADC), NSAW

****
//

3. (U//~~FOUO~~) CRYPTANALYSIS SKILL COMMUNITY PANEL (CASCP) NEWS
by [redacted] Assistant Executive, Cryptanalysis Skill Community Panel

3a. (U) Personnel Change

(U//~~FOUO~~) The Cryptanalysis Skill Community Panel (formerly CA Career Panel) is pleased to announce the following personnel change:

[redacted] (b)(3)-P.L. 86-36
as Director of the CA Skill Community Panel.

[redacted]

3b. (U//[redacted]) Welcome Interns!

(U//[redacted]) The CASCP would like to thank all interviewers and escorts who helped us with the FY2000 and FY2001 hiring process. Over the last year we hired [redacted] people into the CA Program with a variety of degrees; including Anthropology, Biology, Chemistry, Industrial Engineering, Language, Linguistics, Mathematics, Philosophy, Psychology, Statistics, and Textile Sciences. Please welcome:

(b)(3)-P.L. 86-36

[redacted]

****

4. (U) KRYPTOS SOCIETY NEWS

4a. (U//[redacted]) KRYPTOS Society Council Members, 2001

President	[redacted]
President-elect	
Treasurer	
Secretary	
Member-at-large 2000-2001	
Member-at-large 2000-2001	
Member-at-large 2001-2002	
Member-at-large 2001-2002	
AMP Intern Rep	
CMP Intern Rep	
CA Intern Rep	
CA Skill Community (CASCP)	
Awards	
Literature	
Historian	
Membership	
Newsletter Editor	
Programs	
Publicity	
Retired Members	
Webmaster	
KRYPTOS Banquet	
UKLO-3	

4b. (U//[redacted]) KRYPTOS Society 2001 Membership Drive
by [redacted]

(U) Are you interested in cryptanalysis?

(U) Do you like to see technical excellence encouraged and rewarded?

(U) If you answered 'yes' to either of the above, for just $5 you can join the KRYPTOS Society for 2001 and possibly win a $10 gift certificate for Borders Bookstore!

(U//[redacted]) The KRYPTOS Society was established in 1981 to promote interest in cryptanalysis, to provide a focal point for the fields of common interest to cryptanalysts of the National Security Agency, and to promote excellence in the cryptologic community. It has since expanded with chapters at GCHQ and CSE as well.

(U//[redacted]) To join, please fill out the attached form and return it and the $5 dues to any of the following:

[redacted]

(U) You may also join before or after the next KRYPTOS talk which will be held at 1300 on 7 May in Friedman Auditorium. Of the people who have joined by 8 May, 10 lucky people will receive $10 gift certificates to Borders Bookstore!

(b)(3)-P.L. 86-36

[redacted]

(U) If you prefer, please fill out and mail the form below along with $5 to [redacted]

Please tell your friends and co-workers! KRYPTOS is a "learned organization" which limits our ability to advertise this membership drive. Thanks!

~~~~~~

2001 KRYPTOS Society Membership Form

(U//FOUO once filled in)

Name:

Organization: Room Number:

E-mail Address:

Interested in chairing a committee? ____ Yes ____ No

Interested in working on a committee? ____ Yes ____ No

If "Yes", please check committees of interest to you:

___ Where needed

___ Cryptanalytic Literature ___ Membership ___ Awards

___ Distinguished Members ___ Publicity ___ Programs

___ Retired Members ___ Newsletter ___ Social Events

You can list my name on the NSA web. ____ Yes ____ No

~~~~~~

****

////////////

have the privilege of learning cryptography/cryptanalysis from him or hearing his music in the Friedman Auditorium? What about you Dundee Society members who had Mr. Callimahos as an instructor in CA-400, "Intensive Study in Cryptanalysis?" It would be nice to have the traditions created by Mr. Callimahos written down. Are they written somewhere?

6b. (U//[redacted]) Jacqueline Jenkins-Nye, World War II Code breaker
(Excerpts from a Baltimore Sun newspaper obituary, provided by [redacted], President-elect, KRYPTOS Society)

(b)(3)-P.L. 86-36

(U) The 3 April 2000 edition of the Baltimore Sun reported that Jacqueline Jenkins-Nye, a Baltimore native, died at age 79 of cancer.

(U) Jacqueline Jenkins-Nye was recruited by the Navy out of Goucher College, where she was studying math and psychology. Her job was to help crack codes used by the Japanese and Germans during World War II. She became part of an improbable chapter in the annals of American warfare that is drawing renewed interest from historians since the broadcast in November 1999 of a "Nova" special on World War II code breakers. Jacqueline was among a small group of scientifically accomplished "Goucher Girls" the Navy recruited to help crack the seemingly impenetrable Japanese and German codes.

(U) Sworn to secrecy and threatened with death if they spoke of their work, a dozen women from the Class of '42 were recruited for service for, among other things, helping to break the code that enabled U.S. fighter pilots to shoot down and kill Admiral Isoroku Yamamoto, the mastermind of the Japanese attack on Pearl Harbor, in 1943.

(U) In her later years, Jacqueline Jenkins-Nye was probably best known as the mother of Bill Nye, "The Science Guy," star of the off-beat educational series for children formerly broadcast on Maryland Public Television and affiliated stations nationwide. On the wall of his home in Seattle hangs a framed copy of his mother's seventh-grade chemistry test from her elementary school days in Baltimore. She scored 100.

(U) If the lesson of her life means anything, friends and family say, it stands as testament to the importance of education, perseverance and never accepting societal limitations.

(U) Thirty years after earning her degree in psychology from Goucher, Ms. Jenkins-Nye returned to school to earn her Master's and Doctoral degrees in education from George Washington University. She was a substitute teacher in the Washington, D.C. public schools, an adjunct professor at George Washington and a manager or analyst in seven federal agencies from 1968 to 1982. She concluded her career at the National Archives before moving on to start a human resource development consulting firm at age 66.

(U) But perhaps the most intriguing chapter of her life--the three years she spent as an officer in the U.S. Office of Naval Communications--was the one she spoke of least. "We were called down by the dean of Goucher one day, and there were these strange people there who said they wanted us to take some training in a new field called 'cryptanalysis," recalled Fran Suddeth Josephson, 79, now an artist in Summersville, S.C. "They didn't say why, or what it was related to."

(U) The dean's name was Dorothy Stimson. She was the cousin of Henry Stimson, U.S. Secretary of War, who was contacting women's colleges around the country seeking their best and brightest for a project so secret that none of the participants was allowed to know its purpose.

(U) Among the brightest of the lot was Jacquie Jenkins, described by Mrs. Josephson as "Headstrong...maybe a little more independent-minded than the rest." Upon graduation in 1942, the young women were invited to Washington. They were offered commissions in the new branch of the Navy known as the WAVES (Women Accepted for Volunteer Emergency Service). After a whirlwind tour of military training, including practice in wielding cumbersome .45-caliber semiautomic pistols, they returned to Washington and began analyzing intercepted radio transmissions. Even among best friends in the Goucher group, discussion of individual assignments was strictly forbidden.

(U) "None of us ever knew what the others were working on," Josephson recalled. "Only years later, at our reunions, did we ever find out that some of us were assigned to different aspects of the same project. You just never knew."

(U) A few years ago, Bill Nye traveled with his mother to the National Cryptologic Museum near the National Security Agency. He was stunned to see a picture of her unit on the wall.. "I was over in the corner, making all this noise, l ike, 'Jeez, Mom, that's you. That's my Mom," Nye said. "And this tour guide came over, and pretty soon it was quite a scene. All these people were standing around Mom, reading about all these exploits on the displays they have there. It was amazing, and I think very gratifying for her."

****
//

7. (U//[redacted]) KRYPTOS PUZZLES
(by KRYPTOS Puzzle Editors: [redacted]

7a. (U) Solution to "WANT MATH FLEET? FLATTEN WET HAM!"

(U) The puzzle editor who was scheduled to contribute this issue's puzzle was conveniently TDY at the time the puzzle came due. The other two puzzle editors

(b)(3)-P.L. 86-36

[redacted]

would never stoop to embarrassing the missing party by naming names, so they have valiantly stepped in with some crypto-math to save the day. You know what to do:

(U/[redacted]

```
        M A T T                M A T T                M A T T
          x   F A N T E          x   F A N T E          x   F A N T E
          -------------------    -------------------    ---- --------------
             N T M L E                  * * * *
          F A M M H                  * * * * *
         M A T T                     * * * * *
    N M H C L                     * * * * *
    R H E A                       * * * * *
   ----------------------     ---------------------------    ----------------------
  L A C E R A T E        B R E A K F A S T        C O G I T A T E
```

(U) Solution for three multiplications as follows:

	#1	#2	#3
M	3	8	4
A	4	2	7
T	7	4	5
F	2	9	1
N	1	3	6
E	5	1	0
L	8	B - 7	C - 8
H	9	R - 6	O - 3
C	0	K - 5	G - 9
R	6	S - 0	I - 2

(U) Solution:

0	1	2	3	4	5	6	7	8	9
C	N	F	M	A	E	R	T	L	H
S	E	A	N	T	K	R	B	M	F
E	F	I	O	M	T	N	A	C	G

(b)(3)-P.L. 86-36

(U//[redacted] Solvers: [redacted]

7b. (U) New Puzzle: "Jump-All-But-One Game"

(U) I recently returned from a visit to South Carolina. I experienced some down home southern cooking and a particularly good dessert called an "apple dumpling" at a chain restaurant/store called the "Cracker Barrel". Sitting on the table was a little puzzle called the "jump all but one" game. The puzzle was a triangular piece of wood with 15 holes drilled in it. The holes were arranged as shown below.

```
      *
     * *
    * * *
   * * * *
  * * * * *
```

(U) Each hole, save one, had a golf tee inserted into it. The directions printed on the game board stated: "Jump each tee and remove it. Leave only one - you're a genius, leave two and you're purty [sic] smart..." The directions conclude by questioning the intelligence of those who leave three, four, or more tees.

(U) My first try was unsuccessful. After another visit to the Cracker Barrel (and another apple dumpling) I found a solution that leaves only one tee. If we number the holes

```
      1
    2   3
   4  5  6
  7  8  9 10
11 12 13 14 15
```

then a solution is [Leave 1 empty; 4, 1; 6, 4; 1, 6; 7, 2; 13, 4; 10, 8; 2, 7; 7, 9; 15, 13; 12, 14; 6, 13; 14, 12; 11, 13].

(U) This month's puzzle is to diagnose this game; i.e. find all solutions that leave 1 or 2 pegs from the 15 different starting positions.

(U//[redacted] Please send solutions to this puzzle to [redacted] Please send new puzzle ideas to [redacted]

7c. (U) 2000 KRYPTOS KRISTMAS KWIZ Winners

(U) The 2000 KRYPTOS KRISTMAS KWIZ was a great success, despite being done entirely via the KRYPTOS Society website. We received a total of 17 entries (well over double last year's total!).

(U//[redacted] The people who scored at least 50 points on this year's Kwiz are:

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted]

Honorable mention goes to the other contestants: [redacted] (b)(3)-P.L. 86-36

We extend our congratulations to Three Men in a Boat (although we wonder which guy on the team they don't consider a man)! We also congratulate [redacted] on his second place overall finish, and top individual finish!

The answers for this year's Kwiz are available on the KRYPTOS Society website. We expect to receive the 2001 Kwiz in December and we hope everyone will participate again.

****
//

8. (U//FOUO) REAL WORLD CA CHALLENGE: HELP WITH A CODE?
(Request from the Center for Cryptologic History; by Barry D. Carleen, Chief, Publications Center for Cryptologic History)

(U) The Center for Cryptologic History recently received a letter in which the correspondent asked for our assistance in decoding a couple of passages in a Shaker manuscript she was researching. In the words of the letter writer, "The original [manuscript], the Family and Meeting Journal of 1818-1822, is at the Library of Congress, Shaker papers #42, p. 266, microfilm p. 466.

(U) "This particular passage was written in the early 1820s. The author was a Shaker, Isaac Newton Youngs, who was a clockmaker, tailor, mechanic and scribe for the society. Though he was assigned to write this journal, and the Shaker elders had the right to inspect (or confiscate) it, he disguised several passages by coding them--probably more to discourage the elders from reading it, than to prevent them from doing so.

(U) "Probably the topic was sensitive. The easily translatable part discussed Isaac's historical relationship with David [Slosson?], and lapsed into code during a discussion of David's character....In other coded passages, he argued against Shaker doctrine and reported an orchidectomy. But he also encoded words and phrases in uncontroversial passages."

(U) The correspondent has tried various attacks on the code but has been unable to figure it out.

(U//FOUO) If any of our readers are interested in working on this problem, please contact [redacted] at the Center for Cryptologic History. She may be reached at [redacted]

****
//

9. (U) EDITORIAL CORNER

REMINDER: (U) Submissions are welcome at any time. Please feel free to e-mail any input to the Editor, capwils@z.nsa. All submissions must be in ASCII, Frame Maker, or Word Document format, and MUST BE PORTION-MARKED with the appropriate classification. If other than NSA/CSSM 123-2 governs the classifications, please so indicate.

(U) If you have any comments or suggestions, please submit them to any member of the _Tales of the KRYPT_ Editorial Board.

(b)(3)-P.L. 86-36

(U//FOUO) _Tales of the KRYPT_ Editorial Board
Editor: [redacted]
Puzzle Editors: [redacted]

[redacted]

[redacted]

(b)(3)-P.L. 86-36

[redacted]

~~TOP SECRET//COMINT//X1~~

~~(TOUO)~~POCs:

CES External Page
(U) *Last Modified: 10/30/2002 11:42:26*

(b)(3)-P.L. 86-36

Tales of the Krypt - May 2002

Feature Articles

- (U) Editor's Desk - TOTK Survey Results
- (U//~~FOUO~~) Shadowing the SIGINT Director
- (U//~~FOUO~~) CA-400, Intensive Study Course in General Cryptanalysis
  - (U//~~FOUO~~) The CA-400 Experience, or "We Are Slaves to Duty"
  - (U//~~FOUO~~) An Ethos of Kryptos: Lambros Demetrios Callimahos
- (U//~~FOUO~~) Desert Storm: A CA Perspective
- (U//~~FOUO~~) The Story of the Gold Bug
- (U//~~FOUO~~) Principles of Diagnosis

(b)(3)-P.L. 86-36

Regular Features

- (U//~~FOUO~~) Meet the Intern

Editor's Desk - TOTK Survey Results

(U) In January, a new editorial board was formed for Tales of the Krypt and we conducted a survey of the KRYPTOS membership to get a feeling for the kinds of articles people most enjoy as well as for the frequency and method of publication preferred by our readers. Thanks to all who participated, and we hope you enjoy the new TOTK look. Submissions (or suggestions for articles you'd like to read) are welcome at any time. Please feel free to e-mail any input to the Editor, , or to contact any TOTK board member with your ideas. (New board members are also welcome.) Submissions may be in ASCII, Frame Maker, or Word Document format and should be portion-marked with the appropriate classification.

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

(b)(3)-P.L. 86-36

Tales of the KRYPT Board:

- Editor -
- Typesetter and Ass't Editor
- Editorial Board:
  -
  -
  -
  -
  -

(b)(3)-P.L. 86-36

(U) The majority of survey respondants had read the TOTK in the past and were looking forward to reading it in the future. Articles particularly remembered were those of an historical nature (perspectives, seniors' experiences, colorful characters), puzzles and quizzes. When asked what format you wished the new TOTK to be, the great majority preferred either email containing the document in text format, or an email announcement with a table of contents and a link to the KRYPTOS home page. And over half preferred that it be published quarterly.

(U) The top 5 KINDS of articles you want to see in future issues are:

- 1st place - 17 votes - Historical cryptanalytic success
- 2nd place - 14 votes - Biography of a past cryptanalyst of great eccentric renown
- 3rd place - 13 votes - Technical article on current CA work
- 4th place - 12 votes - Biography of a past cryptanalyst of great technical renown

and tied for 5th place with 10 votes each:

- "State of CA" as viewed by an agency senior in the CA field
- Article on current work but with more of a feature/human-interest slant
- Information from the perspective of a former CA'er involved in the larger SIGINT enterprise
- Human interest perspective on a CA conference or event
- Trip reports for CA conferences or other events

(U//~~FOUO~~) In order to respond to the interests of our readers (and, ok, also the interests of the editorial board), in this issue, we bring you one story of an historical cryptanalytic success (CA Perspectives on DESERT STORM) and two articles about Lambros Callimahos and his CA-400 course (this covers both a past cryptanalyst of great eccentric renown and a past cryptanalyst of great technical renown). We also present a set of diagnostic principles compiled by R. Dale Shipp (a recent past cryptanalyst of technical renown), an article by [redacted] about his experience shadowing Maureen Baginski, and an article about the Goldbug (both the award and the original Edgar Allan Poe story), as well as an interview with a current CA intern. - *The Editors*

back to top

(U) Shadowing the SIGINT Director

(b)(3)-P.L. 86-36

by [redacted] (b)(3)-P.L. 86-36

(U//~~FOUO~~) A while back, the SIGINT Director volunteered to share a day with five analysts from the SIGINT Directorate. The plan was for the analyst to shadow Ms. Baginski for a day and then have her follow the analyst for a day. I submitted my name and was selected. My day to shadow Ms. Baginski was 5 February, 2002.

(U//~~FOUO~~) I did not have to begin my day until 7:30. Ms. Baginski begins around 5:00 each day. Ms. Baginski's Executive Assistants told me that the calendar they sent out the previous day was "out the window." There was going to be a guest from Congress arriving the next day and work had to be done to prepare.

(~~S~~) This was the schedule for 5 February. It was a fast-paced day, but here is what stuck in my mind. SIGINT DIRECTOR Tuesday, 5 February 2002:

0700-0730	OFFICE APPOINTMENT
0730-0800	SID SENIOR LEADERSHIP MEETING
0800-0815	DIR'S PREP SESSION FOR CONGRESSIONAL VISIT ON 6 FEB
0830-0915	SIGINT MODELING AND SIMULATION: CONTINUATION MEETING
0930-0955	DISCS ON FOREIGN RELATIONS
1000-1130	SID DIR WITH DDs/CHIEF OF STAFF, SID PROGRAM'S ANNUAL REVIEW BRIEF
1130-1230	WORKFORCE ENGAGEMENT DISCS WITH S111 PERSONNEL
1245-1315	DISCS WITH D/DIR, SID, AND DDDA
1330-1430	PREP SESSION WITH ACTION AND COMMUNICATIONS TEAM
1430-1530	PREP FOR TOWN MTG
1530-1630	DIR'S FINAL PREP FOR 26-27 FEB OFFSITE
1645	DEPART FOR THE DAY

0700-0730 OFFICE APPOINTMENT

(U//~~FOUO~~) Ms. Baginski began the day meeting with her Executive Assistants. She reviewed the Town Meeting agenda and drafted a rough outline for the presentation to the Congressional visitors arriving the following day.

0730-0800 SID SENIOR LEADERSHIP MEETING (b)(3)-P.L. 86-36

[redacted]

(U//~~FOUO~~) The outline for the Congressional presentation was given to the SID leaders. There was some discussion about the outline and goals were set for each stage of the presentaion. A rough draft would be ready by 10:00.

0800-0815 DIR'S PREP SESSION FOR CONGRESSIONAL VISIT ON 6 FEB

(U//~~FOUO~~) My first of two rides in the "special" elevator to the Director's suite. This was a meeting to prepare for the Congressional visit. There were about fifteen people in the room, I recognized only the Director and Ms. Baginski. The objective seemed to be to introduce the Congressional members and their Staff to NSA and SIGINT and help them understand what it takes to keep our mission going. Lieutenant General Hayden knew what he wanted accomplished, picked the people to do it, and guided the discussion.

0830-0915 SIGINT MODELING AND SIMULATION: CONTINUATION MEETING

(U//~~FOUO~~) Too far over my head.

0930-0955 DISCS ON FOREIGN RELATIONS

(~~S//SI~~) Ms. Baginski's meeting with SID and Corporate Foreign Relations managers/representatives. The discussion was about data sharing, both ways, leveraging

[redacted]

1000-1130 SID DIRECTOR WITH THE DDs/CHIEF OF STAFF, SID PROGRAM'S ANNUAL REVIEW BRIEF

(U//~~FOUO~~) This meeting was superseded to prepare for the congressional visit the next day.

(~~S~~) The Data Acquisition, Analysis and Production, and Customer Relations management and staff presented their proposed briefing for the Congressional visit to Ms. Baginski. They were working off the outline Ms. Baginski jotted down at her meeting at the beginning of the day with her Executive Assistants The SID Seniors put together a 20 to 30 slide briefing from the outline. Some of the main points were; the three SID priority focus areas (Defend the nation, Support the campaign, and Transform the SIGINT enterprise), how many reports were derived from SIGINT, NSA's strategic plan, pre and post 11 September SIGINT targeting shifts to support the campaign, and how the extra Counterterrorism money Congress gave NSA was being spent. The first draft had a few holes where actual facts/numbers had to be put in, but in general Ms. Baginski thought things were going in the right direction.

(b) (1)
(b) (3)-P.L. 86-36

1130-1230 WORKFORCE ENGAGEMENT DISCS WITH S111 PERSONNEL

(~~S~~) The best part of the day in my opinion was the meeting with S111. This is the Office which maintains and developes the [redacted]

[redacted]

(b) (3)-P.L. 86-36

[redacted]

[redacted] (U//~~FOUO~~) The [redacted] team was being inundated with queries from several offices. They felt these queries could be consolidated and the offices should take more time to know what they would like to measure and for what reason. They asked Ms. Baginski to help them get this across to the organizations' staff and/or management. (S) Th[redacted] designers had issues with the development of the [redacted] database. They were concerned with the allocation of money, resources, and work roles between [redacted] I believe Ms. Baginski valued this interaction. (Ms. Baginski has had follow-on meetings with the [redacted] office and [redacted] who is supporting [redacted] This topic was also discussed at the Director's offsite on 27 and 28 February.)

1245-1315 DISCS WITH D/DIR, SID, AND DDDA

(b) (3)-P.L. 86-36

(U//~~FOUO~~) I did not attend this meeting. Instead, I observed the formulation of the SID Congressional briefing.

(U//~~FOUO~~) The SID leaders had been working on the brief since the morning meeting. Most of the slides were completed and a few more were added. (When I returned to my office the next day, everybody was talking about what a madhouse it was trying to answer questions for the report.)

(U//~~FOUO~~) I squeezed in time to eat lunch. Ms. Baginski and her Execs ate lunch at their desks sometime after the 12:45 to 1:15 meeting.

1330-1430 PREP SESSION WITH SID ACTION AND COMMUNICATIONS TEAM

(U) This meeting was cancelled to prepare for the Congressional visit the next day.

1430-1530 PREP FOR TOWN MTG THE NEXT DAY

(U//~~FOUO~~) (This was actually the preparation for the Congreesional visit.) Most of the slides were completed and a few more were added. It was still too SIGINTese for Ms. Baginski and many of the slides had too much information. [redacted] from the [redacted] offered help in adding more "flare" to the presentation. His office could add some multi-media, photos, and formatting to the product. Ms. Baginski was getting the impression that SID management was having difficulty collecting the data points needed to support the goals and strategies Congress expected NSA and SID to be addressing.

(U//~~FOUO~~) After a talk with her assistants and some staff members, Ms. Baginski decided to cancel the SID Town Meeting for that day. She was very conciencous about presenting a quality message to the workforce. It was agreed that there was a deadline for the Congressional visitors and they would tackle one thing at a time. The Town meeting was cancelled to work on the Congressional presentation for the following day.

(b) (3)-P.L. 86-36

[redacted]

(b) (3)-P.L. 86-36

1530-1630 DIR'S FINAL PREP FOR 26-27 FEB OFFSITE

(U//~~FOUO~~) I recognized some faces at this meeting, [redacted] My second ride in the "special" elevator to the Director's suite. This was a dry-run for the Senior's Strategic Planning Offsite. There were not many changes to the slides that were handed out at the start of the meeting. Lieutenant General Hayden wanted the slides to reinforce the Agency's goals and leave most of the time to have the Seniors team build. I believe that even less time could have been spent on the slides. Management at that level should have the Agency's Strategic Plan memorized.

1645 DEPART FOR THE DAY

(U//~~FOUO~~) Ms. Baginski had some side meetings afterwards before we returned to her office around 5:15. Her day was not over, but I was allowed to leave. After all that work, the Congressional visit ended up being cancelled late that evening.

(U//~~FOUO~~) My day with Ms. Baginski was inspirational. I believe we have real leadership at the top. They are focused, hard working, know the business, and have a plan. Observing the meetings of SID management, below the SID Director, has also inspired me. I am trying harder to keep management informed. I would have liked to have seen the justification for some of the numbers and data points they presented. Hopefully better dialogue will lead to better quality.

back to top

(U) Desert Storm: A CA Perspective

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

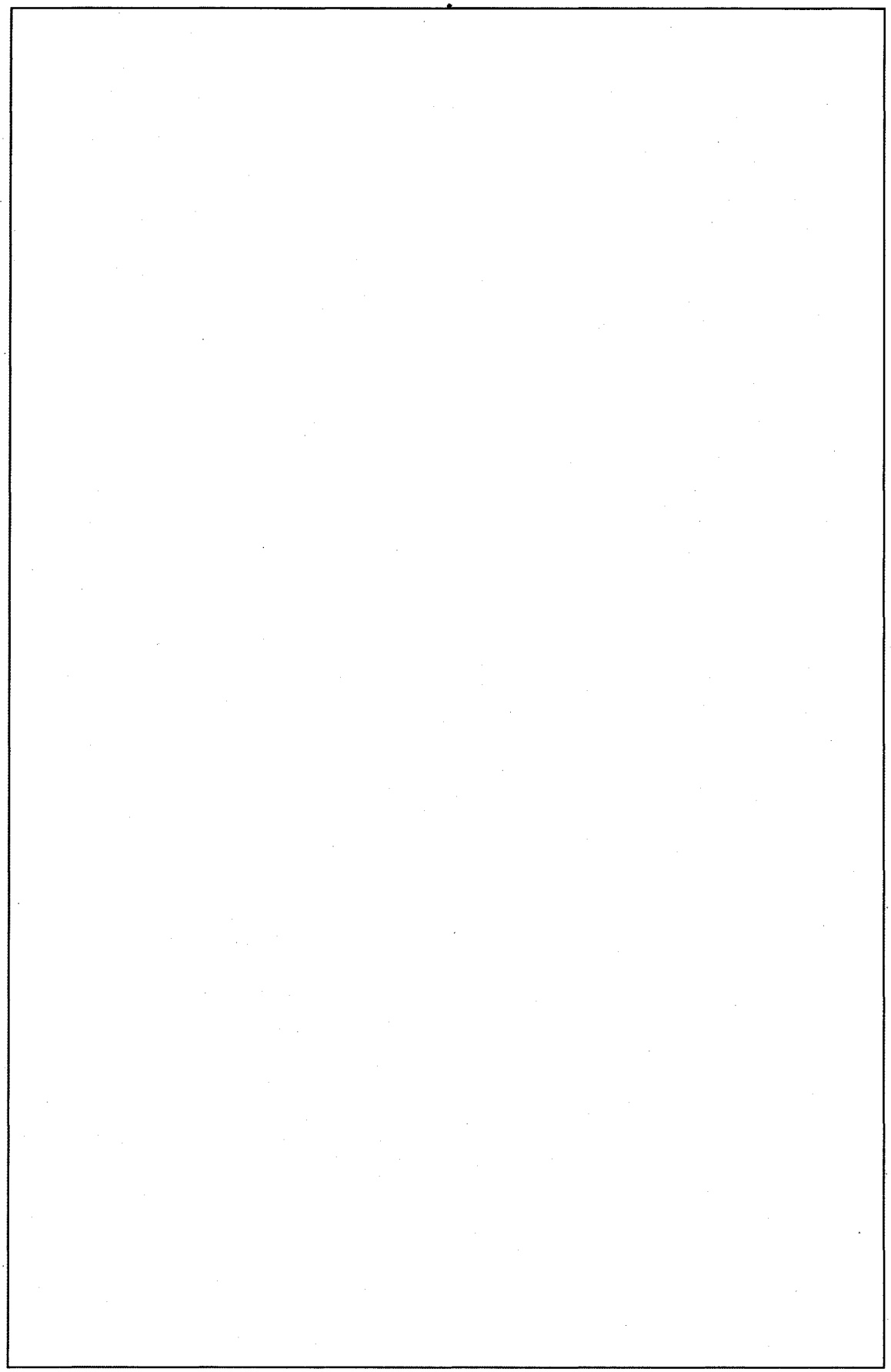
by [redacted] (b) (3)-P.L. 86-36

[redacted]

(b) (3)-P.L. 86-36

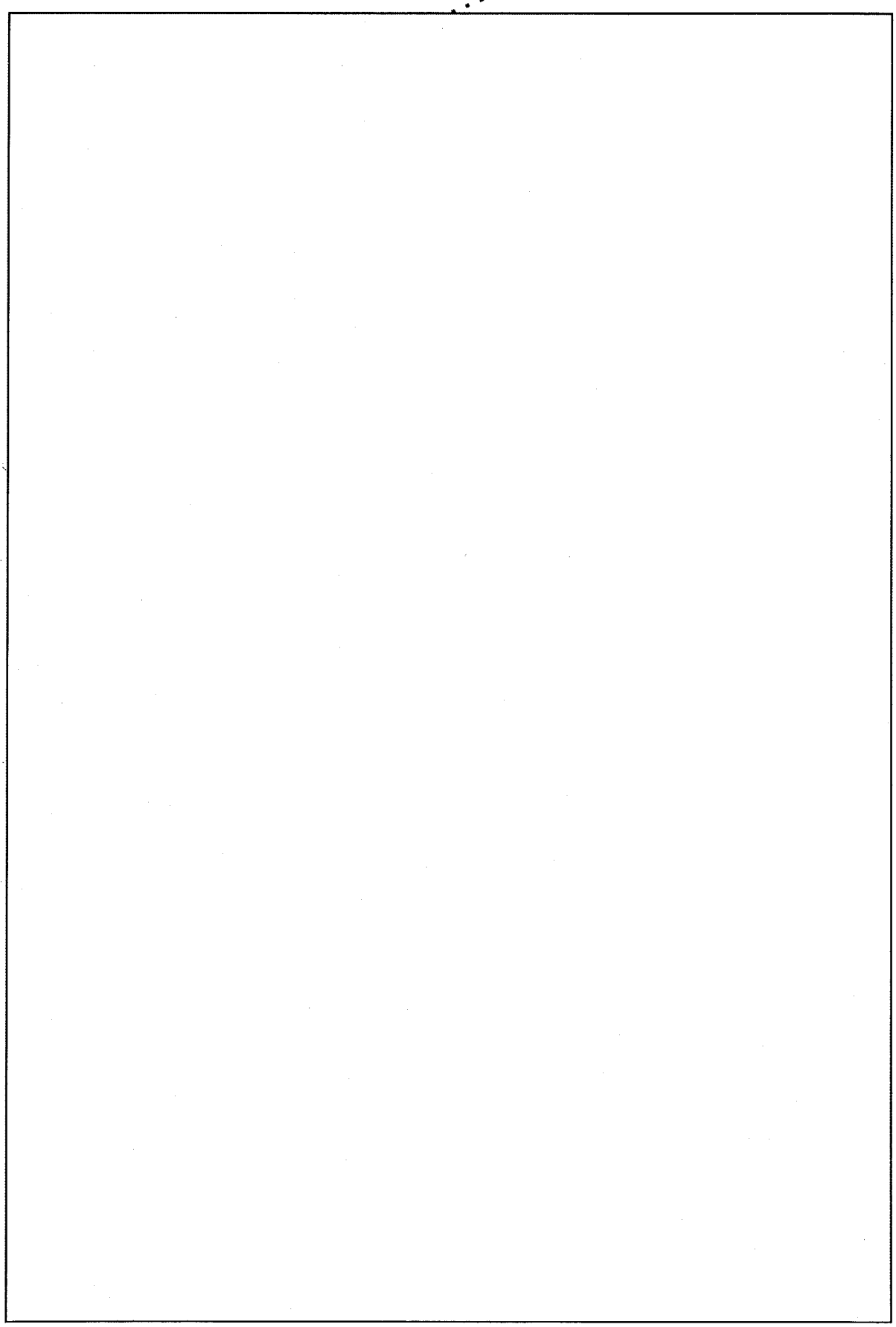
[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



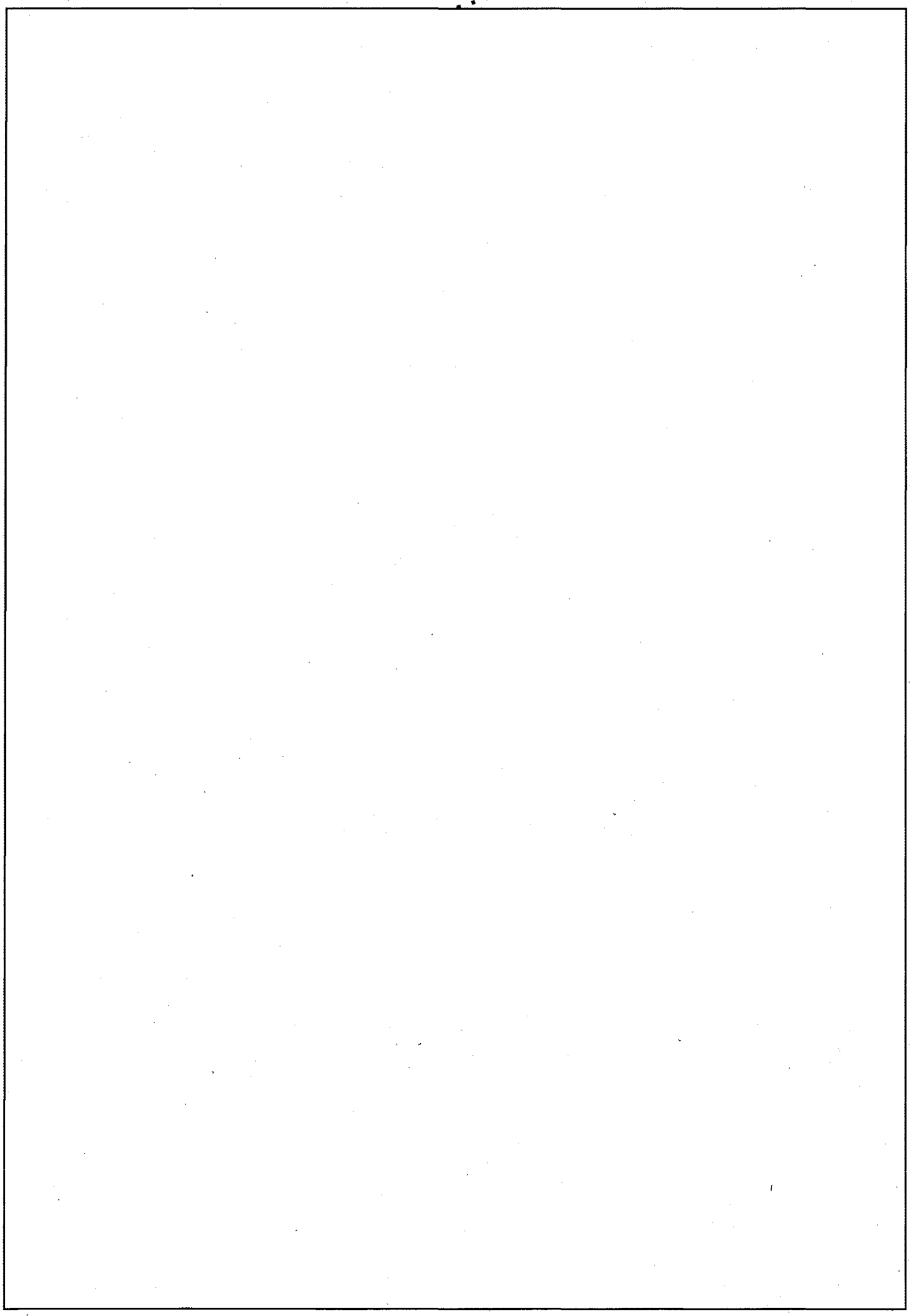
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



(b)(3)-P.L. 86-36

mission, and function statements. He was then selected to be branch chief, a position he held from 1991 to 1997.
back to top

(U//~~FOUO~~) CA-400, Intensive Study Course in General Cryptanalysis

Editors note:

(U//~~FOUO~~) CA-400, the Intensive Study Course in General Cryptanalysis, was developed by Lambros Callimahs almost 50 years ago. During the 33 years when the course was offered, over 300 students were put through this grueling 18-week immersion in classical cryptanalysis. After advancing through progressively more difficult problems, the class was ready to tackle the ultimate challenge: breaking the enciphered communications of Zendia, a fictional country at odds with the Free World and led by Salvo Salasio, who bore an uncanny resemblance to Mr. Callimahos. Beyond developing the students' analytic skills, an important by-product of CA-400 was the spirit of camaraderie and teamwork that started within the confines of each individual class and ultimately extended to encompass all CA-400 graduates (otherwise known as members of the Dundee Society) and the cryptanalytic community at large.

(U//~~FOUO~~) [redacted] a graduate of class 18 in 1964, has written an article about Mr. Callimahos for this issue of Tales of the Krypt. After Mr. Callimahos became ill in 1976, [redacted] assisted him in conducting classes 31 and 32 and became the sole teacher of CA-400 after Mr. Callimahos passed away in October 1977. [redacted] a graduate of class 32, has written a personal account of what it was like to experience CA-400 first hand. [redacted] (b) (6)

[redacted]

The CA-400 Experience, or "We Are Slaves to Duty"

By [redacted] (b) (3)-P.L. 86-36

(U//~~FOUO~~) CA-400, the 4-month long Intensive Study Course in General Cryptanalysis; was rumored to be quite intense, second only to the infamous Managerial Grid. And besides, women who attended it were rumored to have been made honorary men. So what was its attraction?

(U//~~FOUO~~) In 1976, restless and plodding away in one of my less memorable jobs, I saw the CA-400 ad and decided a 4-month break from my office would do me good. I applied and a few weeks later was granted an interview with the course developer and teacher, Mr. Lambros Callimahos. Flanking him was a man I recognized as [redacted], who had once done some analytic programming for my previous team chief.

(U//~~FOUO~~) One thing Mr. C impressed on me was that the course required a full commitment from all participants, and thus the instructor would tolerate no more than one birth, one death, one marriage, one divorce, and one new house purchase from all, not each, but all, of the students! And then they asked me if I were planning to get married. What nerve! "Well, I'm not married now," I snapped. A few weeks later I was

(b) (3)-P.L. 86-36

[redacted]

notified that I'd been accepted into the class.

(U//~~FOUO~~) The first day of class was in early February 1977. I wandered into the classroom and saw two instructor desks and twelve student desks, in three neat rows of four desks each, with a single aisle down the middle. Each student desk had nameplate and a Dundee marmalade jar full of pencils. I read left-to-right and back-to-front the names of 12 students. Mine was the ninth desk, in the back row. There was a 12-hanger coat rack with a label above each hanger. I hung my coat on the ninth hanger.

(U//~~FOUO~~) The room soon filled. Someone complained that her hanger had someone else's coat on it. The coat's owner, in turned, complained that the same thing happened to him. Complaints continued, until we found a chain reaction had been caused by the one person who hadn't noticed the labels. Then Mr. Callimahos entered, escorted by [redacted] and the room got quiet. The year before, Mr. C had been diagnosed with brain cancer, and he wasn't in his full vigor, but that did not matter. We were in awe and sat quaking in our proverbial boots.

(U//~~FOUO~~) Role call was done in order, from student #1 through student #12. "Sister [redacted]?" "Here!" "Brother [redacted]" "Here!" Yes, we were "Sister" and "Brother" in that class. At least we did not have to quibble about the variety of feminine honorifics.

(b) (3)-P.L. 86-36

(U//~~FOUO~~) Then Mr. C started reading. Reading, reading, reading. Talking and reading. Hours passed. Finally [redacted] leaned over and whispered something. "Oh," Mr. C exclaimed, "Does anyone have to go potty?" There was a sudden, stunned silence. Then we all ran for the door.

(U//~~FOUO~~) As the days passed a pattern appeared. Mr. Callimahos would enter, sit, and read or lecture. We would attempt to keep pace and work on problems they were encountered. While the Guru went on, [redacted] distributed handouts, some displaying the results of statistical tests, others showing the text in a different format, and so on. My impression was that [redacted] was the highest paid flunky I'd ever seen.

(U//~~FOUO~~) Although we received lectures on new topics, most of our learning was to come from being exposed to the problems and then coached and prodded to sort out the solution. We were encouraged to share our findings and learn from each other. Mr. C would often entertain us with jokes and stories. Sometimes they conjured up a vivid image, and as one of the later-shift students, I often took advantage of the quiet room and empty blackboard and... sort of... left a little illustration. Once it was a Guru Special, a sandwich made up of his most colorful gastronomical favorites. Another time it was the Guru riding a Big Wheel (wired of course) with the class bowing in awe. Then there was the class on a train, the class on a hayride, the class playing baseball, the class performing "The Pirates of Penzance." The first illustrations were met with gasps from the Guru and his minion. Who could would be so cheeky as to touch their board after hours?! But after a while they got used to not knowing quite what to expect from Class 32.

(U//~~FOUO~~) As the weeks went on, our class got more and more cohesive. We learned how to solve problems by working together. In some places this is called "cheating." Here it was called "teamwork." But something else happened. We, the students, slowly took over the class.

(b) (3)-P.L. 86-36

[redacted]

(U//FOUO) Maybe it started when Mr. C at last realized that he hadn't yet made the women honorary men. A man of the Old School, he felt this was the only way he could tell his off-color jokes. Well, this was 1977, the height of this era's feminist movement. We nipped that idea in the bud. "Mr. C if you make us honorary men, we'll have to make you an honorary woman." Then the names; "Sister [redacted] made me feel as if I had just got off the boat from an Irish nunnery. We ditched the last names, but amusingly still, kept the titles, and became Brother [redacted], Sister [redacted], etc. And then the unthinkable! We made [redacted] an honorary member of class 32. The Guru's devoted wife would bring him to work and pick him up. We often escorted him to the car (thus eliminating one of [redacted] jobs) and quickly came to like and admire her. It was Brother Joe who first noticed it my drawings: where we students started out in positions of servitude and awe, we were later to be seen running totally amuck, with an astonished Guru (and assistant) looking on helplessly.

(b) (3) -P.L. 86-36

(U//FOUO) Indeed, during the course of CA-400 class 32 a Baby [redacted] was born. Sister [redacted] moved house. One divorce was initiated and one marriage resulted. And sadly, most sadly, it turned out to be the Guru's last class.

An Ethos of Kryptos: Lambros Demetrios Callimahos

By [redacted]

What is the plural of sphinx? And how would you order two of them? Can you name the ten champagne bottle sizes? What was Frederick the Great famous for? And who was the J. J. Quantz hiding in his closet? Give four reasons why George Washington was not a good flutist.

If you ever wandered through the wonderland of the Callimahos Course you might have bumped into the answers to some of these questions-and many more that students of four classes of the 'Callimahos Course' compiled from his mutterings. Mr. Callimahos, as many of us knew him, was the Keeper of the Keys to the Cultural World of Cryptanalysis as we knew it. He introduced us to Jean Francois Champollion, who didn't need Callimahos to learn about the value of isolog - or isologues, as they are known in England. We saw Zendia through his eyes; the music of Josef Pujol became harmonious memories (those tetra-chords!) for us. We found out about the Gourmet Club-the difference between cooked lamb's eyes and fish eyes, (as well as medium-rare rhinoceros meat and well-done elephant meat) gastronomically speaking. We gained a perspective of inventors and who invented what in a few of the surprises in the history of inventions.

Callimahos touched on perfumery: little-known aspects of that old industry still quite active in his birthplace. His interest in this subject may have sparked his interest in pet skunks he would frolic with unprotected on his front lawn! And what bubbles can you burst with Buffont's needle?

Lambros Demetrios Callimahos, one of the founders of the Cryptomathematics Institute, was born on December 16, 1910 in Cairo, Egypt, of Greek and Armenian parents. He was a flute virtuoso, known as the 'Paganini of the flute'. Callimahos toured Europe in the years before World War 11, ending up at Carnegie Hall, where he performed as a solo artist-a first at that great center of culture. He began his service with the U.S. Government at the beginning of World War II, when he appeared at his draft board dressed in a way

(b) (3)-P.L. 86-36

he could not be overlooked! And throughout his career at the Agency and its predecessors he could not be overlooked.

He once mentioned that while he was in the army, he shared a BOQ room with a young Lieutenant, Leonard Rosenberg (a.k.a. Tony Randall)! As he remarked, "He was a queer duck, always dressed in spats," some of us wondered (and still do) what Tony Randall's thoughts about his world renowned flutist roommate were. Was this a precursor to "The Odd Couple," or what?

His performances in the form of flute concerts and lectures at the Friedman Auditorium were always to packed-houses. He gave talks about "Beauty in Mathematics," "on Pi," "Communication with Extraterrestrials," and "The Rosetta Stone." He also frequently gave a talk entitled "The History of Cryptology," which he gave several times to Police Academy graduates and other audiences. A prolific author, he received the first NSA Cryptologic Literature Award shortly before he died in October 1977.

Callimahos was best known at the Agency for his "Intensive Study Program in General Cryptanalysis", which he created as an adjunct to his writing. Callimahos had been selftaught by reading all the books he could find - in any language about cryptanalysis, and after he joined the Army he became one of Friedman's students. He collaborated with Friedman in rewriting Friedman's earlier texts, Military Cryptanalysis, vols. I and II. Callimahos added significant portions, especially to volume 11, where he added the Zendian Problem. Just before Callimahos died he published Military Cryptanalytics, Part III the first part of which was based on Friedman's earlier Cryptanalysis, Volume III Friedman also wrote Military Cryptanalysis, vol. IV. Callimahos had also written - but only in his mind - Military Cryptanalytics, Part V, and was ready to put pen to paper had his body only been capable of it. Their plan originally was to publish six volumes: The sixth was to deal with cipher machines, but even in their day that topic quickly exploded in complexity and variety, keeping apace with technology which made it too magnum an opus for them.

We never saw what Callimahos had in store for us in the diplomatic phase of the Zendian Problem; but you can be sure that many of the remarks of the exalted Guru, many of the crafty trivialities of life, and much care would have been built into it. He would have kept us smiling as we set to work.

Kryptos members have a keen sense of wanting to solve it, to sort it all out to the last detail, to master the problem whatever it is. Therefore, I provide you with the infamous "Dundee Society Introductory Placement Test", which encapsulated at least an iota of the emanations of our Guru as we worked through the problems of his course. I will tell you that I am not sure of all the answers to the questions, but I did at least try (once) to record them for posterity. He and I were sitting under the umbrella in his sunny back garden in New Carrollton, with some unremembered libations, and I read each question to him. He dutifully responded with at least one, but often many words to answer the questions.

If I were to do it today, I'd have a recorder to capture it all. But the best I could do was to scribble a few notes on the paper that was already filled with the questions. I can't find those notes now, but maybe that's best. I know you'll all want to know if you got the correct answers. I don't have them all - the only hope you have of being sure you have them right is to get together with your colleagues and a few of us old-timers who heard the quips in the first place, put your heads together, bash it out on the internet, share your

(b)(3)-P.L. 86-36

9/24/2010

work with others, and when you've got it right, you'll know it! And you will have had to do it the way he intended: through teamwork.

By the way, if you want to find out more about Larnbros Demetrios Callimahos, you can visit the web page of Andrew Callimahos, his son, who has many memorable pictures and facts about his famous father. Through that web site you can also learn how to obtain cd's of Lainbros playing the flute. The URL is http://www.geocities.com/callimahos/

Dundee Society Introductory Placement Test

(Culled from parenthetical asides of the Guru by members of Class Nos. 17-20)

1. What is the plural of Sphinx? How would you order two of them?
2. Quote a famous line from Dante in the Italian
3. How do you pronounce "bezoar"? What is its adjectival form?
4. What are the first 10 digits of pi after the decimal point? What are the last 10 digits, when it is carried out to 100,000 decimals?
5. Why, loosely speaking, is Toots Shor not abarticular?
6. Name the seven provinces of Rumania prior to World War II
7. Give the date when combination snuff boxes and slide rules first appeared (a) in England, (b) in France.
8. Is masulipatam cheap or expensive?
9. What is ylang-ylang?
10. What pejorative was applied to Queen Charlotte? Did it redden the skin?
11. Rosehip is often combined with what for what?
12. Who wrote his name on the hem of Mrs. Siddons' garment?
13. Define the following: (a) bdellium, (b) callipygian, (c) logogoguery, (d) monopsony, (e) tachydactylurgic.
14. How do you pronounce (a) "vagaries (b) "harassing"?
15. Do you now or have you ever indulged in (a) sternutation, omphaloskepsis?
16. What or where is Zmudz? How about Yakut and Xosa?
17. Who or what is or was Nicholas Bourbaki?
18. Give the adjectival forms of the following: (a) tergiversation (b) protocol, (c) sable, (d) wife, (e) Jynx.
19. Frederick the Great is best known for what? And who was the J. J. Quantz hiding in his closet?
20. Ptolemy XIII was famous for what three things? What was his appellation?
21. Define I'metheglin" and give its etymology.
22. What is a Singapore chair?
23. Powdered rhinoceros horn is prized for what where?
24. Give the names of the ten champagne bottle-sizes, in ascending order of size.
25. Complete the equation $e^{i(pi)} + 1$
26. Is well-done elephant preferable to medium-rare hippopotamus? Why?
27. What is the difference between cooked lamb's eyes and fish eyes, (a) in appearance, (b) in taste? Are the lenses edible?
28. Give the age of the earth, to two significant digits.
29. Give the correct term for an expert on dolphins.
30. Give the Greek equivalent cited by Mencken for "hundinacido."
31. What is the star nearest our solar system and how far is it?
32. What is the population of Calcutta? How much of it smells?

(b)(3)-P.L. 86-36

33. What is (a) a Prince Rupert drop, (b) a Zamboni dry pile, (c) a rotifer?
34. What work of Mozart's is cited in mathematical bibliographies?
35. After World War I, what was the name of (a) Lemberg, (b) Revel, (c) Dorpat?
36. What was the former term for Down's syndrome? Why was it changed?
37. For what three events is December 16 famous?
38. What is "Eddington's principle"?
39. By the latest count how many atoms are there in the universe?
40. Besides that, for what was Casanova famous?
41. How many angels can dance on the point of a needle?
42. Give a saucy synonym for "crib."
43. How do you pronounce the plural of generatrix?
44. Give the order of ingredients for a typical pousse-cafe.
45. What is the red variety of retsina called?
46. What is the longest word in English without any repeated letters?
47. What is the only word in a Romance language which contains QU not followed by a vowel?
48. Who is the reputed discoverer of Zendia? Who really discovered it?
49. Who is the inventor of the concertina? What did he not invent?
50. Dr. Jacques Loeb did what when where for the first time?
51. Quote a particularly succulent gastronomic item from the U. S Army's "Arctic Manual."
52. What happens when a hydra mother-to-be is temporarily deprived of food?
53. Give the German equivalent for "the early bird catches the worm."
54. Do not give the English equivalent of "le mot du Cambronne."
55. What instrument did Frederic Chopin's father play, and in what business was he that left him stranded in Warsaw?
56. What instrument did Nero play?
57. True or false: more than one tone can be played simultaneously on the flute.
58. What did Paul Wittgenstein and Count Rebsomen have in common?
59. What are the Duke of Brunswick and Count Isouard famous for?
60. What are the former popular names for (a) lead acetate, (b) sulphuric acid, (c) copper sulphate, (d) hydrochloric acid, (e) nitric acid.
61. What is lunar caustic and what was it used for?
62. The Allgaier and Muzio are related in what way?
63. What are the five "K's" of the Sikhs?
64. Give the Hindustani equivalents of "water" and "bread."
65. The last Anarchist Congress held in Brussels in 1914 was conducted entirely in what language?
66. Give the names of two famous coffee liqueurs.
67. What are the four classic fixatives used in perfumery?
68. Explain "Loncls Relativity Constant" without going into too much detail.
69. Why is it called "Goldbach's notorious conjecture"?
70. What was "Project Ozma"?
71. Give the approximate area and population of Zendia.
72. What was M. Lissajous' first name?
73. What was Berlioz's first name?
74. What is a palliative for scleronychia?
75. Give three reasons why George Washington wasn't a good flute player.
76. What is the life expectancy of a Kapitza battery? Why?
77. Describe the opening scene from a typical Helen Twelvetrees movie.
78. In bird groupings, it is a gaggle of geese,

(b)(3)-P.L. 86-36

9/24/2010

a ---------- of rooks,
a ---------- of hawks,
a ---------- of peacocks,
a ---------- of herons.

79. What is a Peaucellier cell?
80. Describe (a) a Wimshurst machine, (b) a Toepler-Holtz machine.
81. What famous cryptologist went to West Point? Why was he bounced?
82. Where is "Sheshach" mentioned in the Bible? What was it? Explain.
83. What is the antonym of nyctalopia?
84. Explain the difference between naology and nanology.
85. What Greek society in New York City never advertises in American papers?
86. Where was Brahms much in demand as a pianist at the age of 10?
87. How many children did Johann Sebastian Bach have ?
88. What was Paganini's son's full name, and who was his mother?
89. What was Heinrich Schliemann's second wife's maiden name?
90. Who transcribed Bach's Chaconne for (a) I hand, (b) 2 hands, (c) 4 hands?
91. Where is Sawedwadgeorgeearllittnbulwig mentioned?
92. What was George Bryan Brummel's father's occupation?
93. Explain the difference between the golden number and the golden section.
94. Give the title of a movie starring Cecile Aubry. By the way, who was she?
95. Name a book written by Cesare Lombroso's daughter.
96. What is the bacillus causing fermentation of yogurt?
97. Describe Jean Francois Champollion's eyes.
98. Give the title of a book written by the inventor of the camera obscura.
99. Is an abacus major an apprentice abacist?
100. Is cochineal silver-grey, black, or red?

back to top

(U) The Story of the Gold Bug

by [redacted] (b) (3)-P.L. 86-36

(U) Edgar Allan Poe's stories of murder, madness and supernatural horror have made him one of the world's most popular authors. "The Gold-Bug", however, is not one of those stories.

(U) It is the story of one William Legrand, formerly wealthy but now poor and reduced to living in a hut on an island near Charleston, South Carolina. The story's nameless narrator, who is Legrand's friend, describes him as "well educated, with unusual powers of mind, but infected with misanthropy, and subject to perverse moods of alternate enthusiasm and melancholy." Among his interests are collecting specimens of the local insects, which is how he finds the Gold Bug.

(U) One day, during an autumn day of "remarkable chilliness", the narrator visits Legrand, who tells him of a "scarabaeus" (That's right, a scarab!) he has recently discovered. Since the bug has unfortunately been lent to another, Legrand makes a sketch of the bug and hands it to the narrator, who tells his friend that he has drawn a skull.

(b) (3)-P.L. 86-36

[redacted]

Miffed at having his draftsmanship slighted, Legrand takes the sketch, examines it, then suddenly folds it up and puts it away. For the rest of the visit, Legrand is increasingly lost in thought, and the narrator finally decides to leave him.

(U) A month later, the narrator encounters Legrand's servant, Jupiter, who tells the narrator that Legrand has been acting strangely, wandering about the island, keeping a slate with strange figures on it, and talking about gold in his sleep. Jupiter blames the bug for this, saying that it bit Legrand when Legrand first tried to capture it. He also has a note from Legrand, stating that he "has had great cause for anxiety", has "not been well lately" and wishes the narrator to visit him that night. Accompanying Jupiter to the island, the narrator sees a collection of digging tools Legrand has ordered bought.

(U) When the narrator arrives, Legrand shows him the gold bug itself, whose shell is a shiny gold color, and has two black spots on one end of its back and a longer spot in the other, giving it a resemblance to a skull. It is tied to a length of cord, and Legrand is swinging it around, claiming that the bug will be his fortune.

(U) Legrand, the narrator and Jupiter go off at Legrand's direction through the mainland until they come to a large tree by early evening. Jupiter climbs the tree at Legrand's direction and eventually finds a skull nailed to the end of a tree branch. Dangling the bug through one of the eye sockets gives the eventual location of a buried treasure chest.

(U) When the treasure is recovered, Legrand explains how it was done. The parchment on which Legrand had sketched the gold bug on turned out to have the enciphered directions to the treasure written on the back in an invisible ink which only appears when heated. The cipher is a simple substitution cipher (about as difficult as the Headline Puzzle). Legrand, having read the message, then spent several days looking for and finding the location as described in the message, at which point he sent Jupiter to Charleston to buy digging tools, and the rest is known.

(U) What is interesting here is Poe's explication of the cipher analysis. Legrand reasoned that the figure of the skull was evidence of the parchment being made by a pirate, and that a sketch of a young goat's head was a signature for the infamous Captain Kidd (Get it?), and that therefore the underlying language was probably English. Of special interest here is that Poe, through Legrand, explains the principles of solving the cipher, first by counting the number of times a character occurs in the message and matching the observed frequencies with the frequencies of letters in English. Poe shows the actual observed frequencies and demonstrates some early recoveries, although his listing of the frequencies of English letters is different from the classic "ETAIONSHRDLU" order.

(U) Finally, Legrand explains that he used the bug as a prop on the expedition to tease the narrator with the possibility that he, Legrand, was insane. (U) The cryptanalysis aside, this is actually one of Poe's weaker stories. The Gold Bug itself is mostly a prop, and the story depends on a string of coincidences whose probability is on a par with winning lottery tickets. The parchment containing the message is found by Jupiter when he looks for something to wrap the bug to capture it. Legrand just happens have the parchment handy when he sketches the bug, and the sketch is in exactly the same spot as the skull drawn on the other side of the parchment. The bug's gold coloring is complemented by its apparent weight, which suggests to the narrator a body of solid gold. The bug's resemblance to a skull is meant to suggest pirates. Poe does everything but give it an eye-patch and peg-leg. And as Poe stories go, being doomed to a lifetime of fabulous wealth

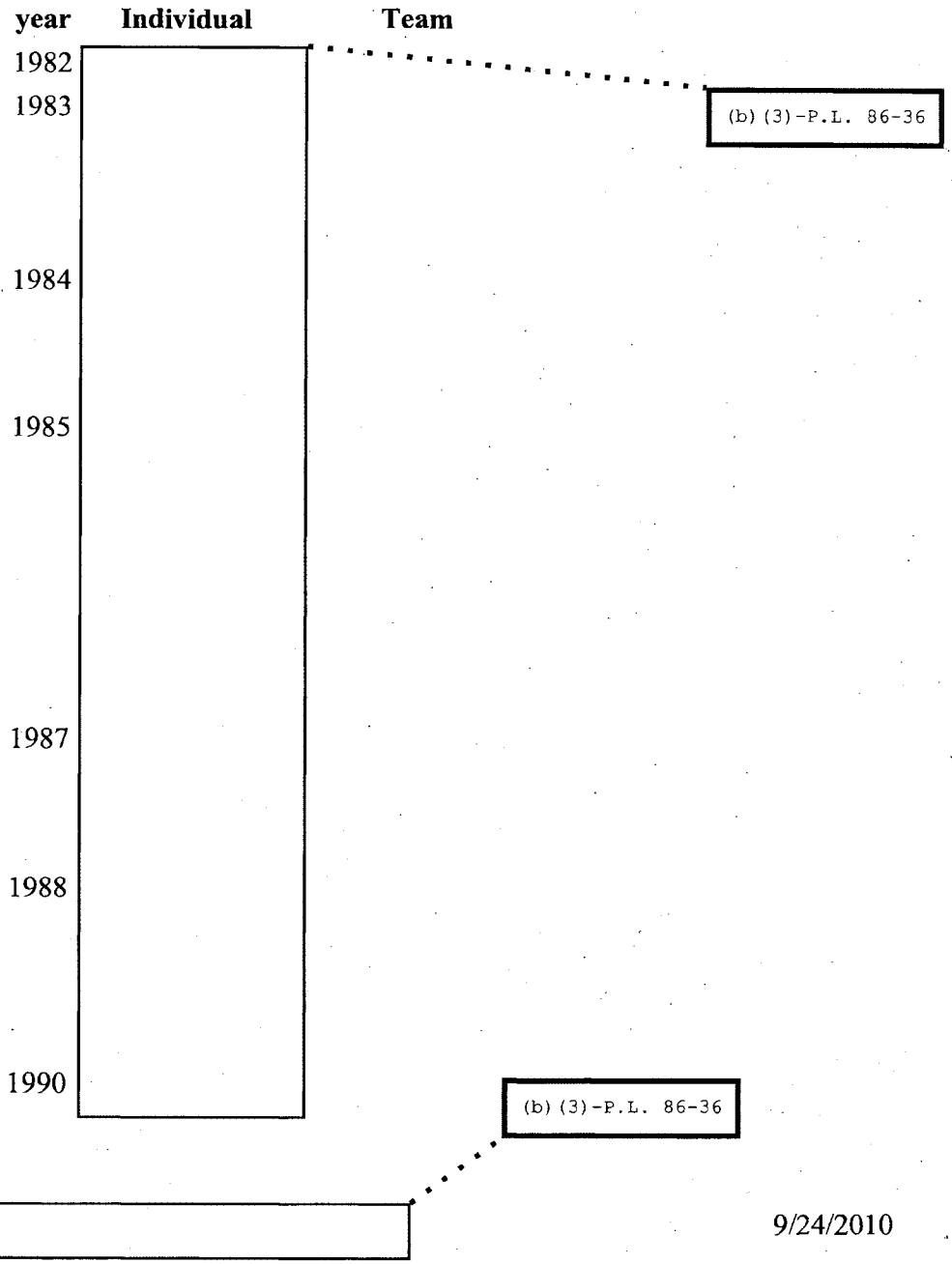
(b)(3)-P.L. 86-36

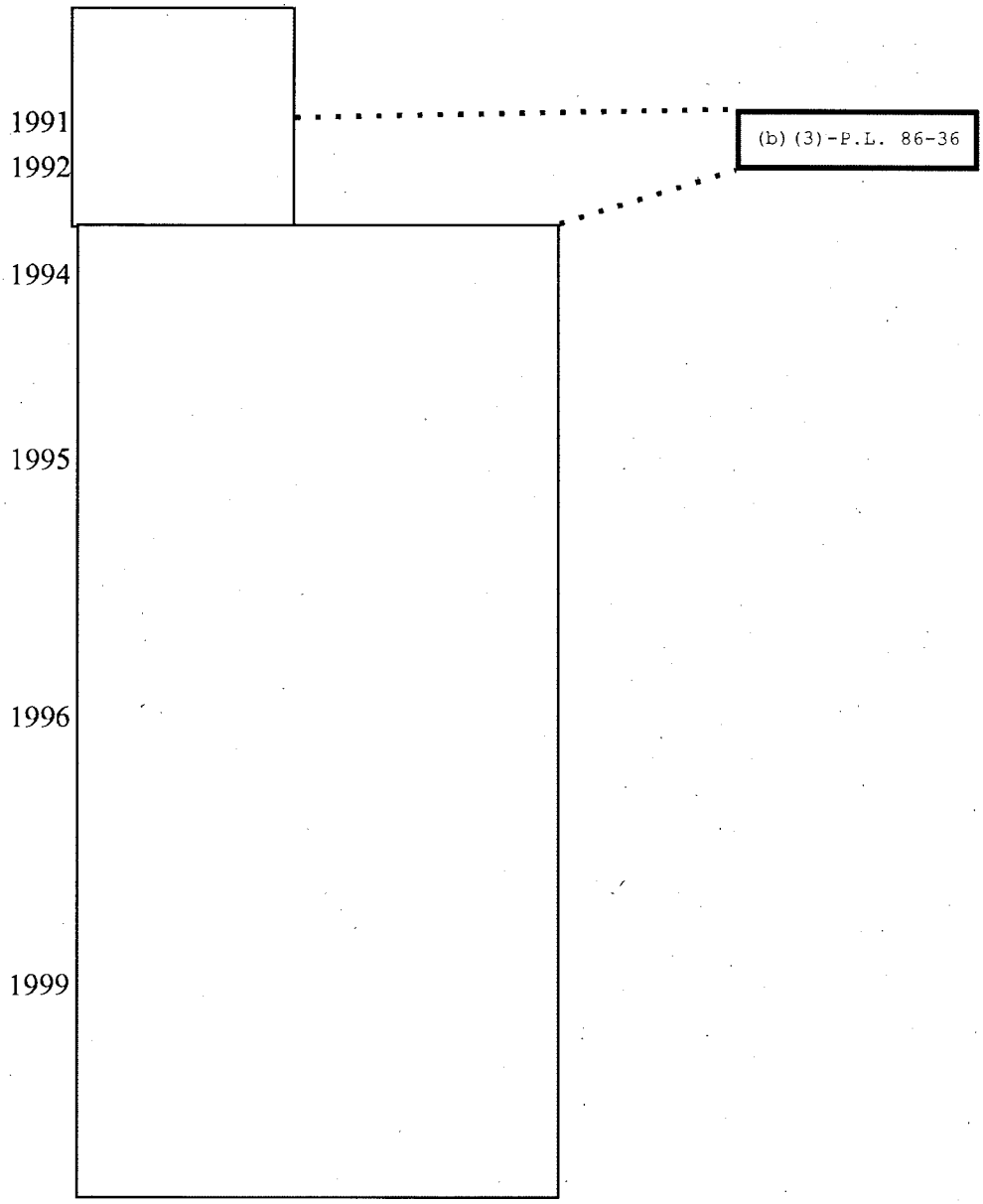
isn't as gruesome as the endings of "The Tell-tale Heart" or "The Masque of the Red Death".

(U) The treatment of Jupiter also mars the story. Jupiter is a walking, dialect-spouting stereotype. Legrand variously berates and threatens him when the mood strikes him. This actually led to an OEO complaint being lodged against the award back in the early nineties.

~~(TS//SI)~~ The Gold Bug Award was established in 1982 by James Bates, then the Chairman of the CA Career Panel. The award is given to honor "outstanding achievement in the field of cryptanalysis." The Team Award was established in 1994. The award is typically given for feats of diagnosis, but it has also been given for attack development, development of new techniques in the course of analysis and, in a few cases, contributions to the COMSEC or INFOSEC effort. A plaque with the names of all past award winners can be found near the elevators in Ops. 2B.

(U) Gold Bug Award Winners





back to top

(U) Principles of Diagnosis

(U//~~FOUO~~) These principles of cryptanalytic diagnosis were gathered by R. Dale Shipp, a Distinguished Member of the KRYPTOS Society (1999). Except for the first, they are not in order of importance. Where known, the originator or popularizer of the principle is credited.

(U//~~FOUO~~) A short bio for Dale may be found in the November 1999 issue of Tales of the KRYPT: http://www.[redacted]nsa/kryptos/Newsletters/1999/nov99[redacted]html

1. (U) Look at the data.

(b)(3)-P.L. 86-36

[redacted]

(U//~~FOUO~~) Corollary: It might be plaintext.

(U//~~FOUO~~) Too often in this modern world, we rely on programs to analyze data and extract preprogrammed features. The human eye and brain are powerful tools that see things that have not been programmed for. Examples exist where direct visualization were of direct importance in successful diagnosis.

2. (U) Let the data tell you what to do. (A Jim Bates saying.)

   (U//~~FOUO~~) When you see an effect in the data that is statistically significant, listen to it. It needs to be explained or expanded.

3. (U) Remember that diagnosticians do not know what they are doing.

   (U//~~FOUO~~) When doing attack development, you usually have a complete model and can evaluate exactly what the scores are telling you. Since you know what the correct answer should look like, you can aford to reach deep into the noise to pull it out using elaborate secondary tests. You can afford to ignore other high random scores which do not fit the known model.

   (U//~~FOUO~~) When doing diagnosis, you have only models that you have invented based upon incomplete knowledge or even speculation. There may well be effects caused by things you do not know. When designing attacks, you should consider statistics that do not depend too deeply on the specifics of your model. I call these "robust statistics". You must be prepared to observe and examine interesting scores that are different from exactly what you were testing for. You cannot often afford to spend significant resouces digging deep into the noise. Your time and energy are better spent designing new models and attacks against them.

4. (U) Use all of the data you can afford.

   (U//~~FOUO~~) This is related to the point above. When doing attack development, you can usually evaluate the amount of data needed to produce the desired result. The use of more data often carries a cost of processing, and may well not add significantly to the chances of success. In any case, because you know what you are doing, you can evaluate both the cost of using the additional data and the gain in success arising from doing so.

   (U//~~FOUO~~) Since the diagnostician does not know the underlying truth, she cannot evaluate normally evaluate with certainty the gain in success arising from the use of additional data, nor the loss resulting from not using it. Often the curve of success versus data size has a sharp knee. Depending where one is on that curve a doubling of the data size may increase chances of success by a miniscule amount (e.g. from nil to almost never, or from .99 to .999) or by a significant amount (e.g. from .1 to .8). We cannot afford to take the chance on being on the wrong side of the later possibility.

5. (U) Do not worry that you will not understand the meaning of a result from a diagnostic run. Do worry about being able to determine the significance of an answer.

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(TS//SI) The best example of this principle comes from a historical antedote. Once when proposing [redacted]

[redacted]

(U//FOUO) We do tests that have been successful at uncovering statistically interesting and relevant phenomena in the past. So long as the current knowledge of the system does not imply failure of the tests, it may well make sense to apply them -- even if we do not immediately understand what the results would mean.

(U//FOUO) The type of tests that are of more dubious value are those for which we are unable to decide whether a result is statistically interesting or not. If we are unable to make this evaluation by either mathematical analysis or simulation modeling, then the value of the test is highly suspect.

6. (U) Data quality is important.

(U//FOUO) This is more true for diagnosticians than for those who are doing exploitation, but true for both. When the goal is to turn cipher into plain on a know system, garbles can often be tolerated and compenstated for. Many diagnostic attacks have combinatorial aspects to them that can be devasted by garbles. Even more common is that many times diagnosticians have had to first diagnose things that we ourselves had done to the cipher at some stage in its processing.

7. (U) Know the quality of your data.

(U//FOUO) Knowledge of the quality of the data is perhaps as important as the quality itself. By understanding the various processing steps and knowing what could have gone wrong -- you are better prepared to understand the results of your tests, and the limitations of them.

8. (U) Believe in yourself and have confidence that you can succeed.

(U) If you do not believe that anything will work, then nothing you devise will work and you are only going through the motions. You need to have an inner sense that the the answer is there, and that you will be able to find it and to recognize its signs. Persistence and imagination have overcome difficult odds.

(b)(1)
(b)(3)-P.L. 86-36

9. (U) Put yourself in a position to be lucky. (Another Jim Bates saying.)

(S//SI) Even when you have little hope for success, keep something going. If you [redacted]

(b)(3)-P.L. 86-36

[redacted]

~~(S//SI)~~ Be prepared to capitalize on good fortune when it comes your way -- but do not sit around waiting for it either.

10. (U) Cooperate and share data and information and ideas.

    (U) This has got to be one of the most important prinicples and values. Very few successes come as the result of sole individual effort.

    (U) No one person nor organization owns the data. Chances for success are enhanced when the data is made available to those who can work on it and contribute, and when all relevant information about the data is shared.

    (U) The creative process thrives on diaglog. By sharing results and ideas, even the half baked ones, we spark ideas in others and lead to more progress on our problem and on other problems.

11. (U) Document and publish.

    (U) Too often, those who have been successful at diagnosis have not published how they achieved that success and only the fact of the success and the result are published. This robs the more junior analysts of a chance for growth. Those who were primarily observers in a successful important diagnosis can contribute to the lore by writing a history of what they saw so that others can see and know the paths that led to success.

back to top

(b)(3)-P.L. 86-36

(b)(6)

(U) Meet the Intern -

(U//~~FOUO~~) started at the Agency in July 2001

~~(S//SI)~~ Before arriving, did have a mildly Hollywood perspective of the Agency. However her training and our beaucracy rapidly changed that! After completing her initial course work (shortly after September 11) she took her first CA tour on the

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36
(b)(6)

(b) (3)-P.L. 86-36
(b) (6)

[redacted]

Meet the Intern *is, hopefully, a regular feature of TOTK. Individuals are encouraged to interview Cryptanalysis interns and send contributions to* [redacted] *for publication in this forum. This feature is meant to be informative and light, if not outright funny... never degrading.*

back to top

(b) (3)-P.L. 86-36

DERIVED FROM: NSA/CSS MANUAL 123-2
DATED: 24 FEB 1998
DECLASSIFY ON: X1

~~TOP SECRET//X1~~

(b) (3)-P.L. 86-36

[redacted]

~~TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, AND NZL//X1~~

Tales of the Krypt - November 2002

POCs: [redacted]
CES External Page
Last modified: Fri Nov 15 11:53:22 EST 2002

Feature Articles

- (U) Diagnosis: Concern and a Turning Point
- (U) CA Intern New Hire Update
- (U) CA Curriculum Review
- (U//~~FOUO~~) A Cryppie's View from [redacted]
- (U//~~FOUO~~) Metadata Analysis Center
- (U//~~FOUO~~) Network Analysis Center
- (U//~~FOUO~~) F6 as an Intern
- (U//~~FOUO~~) My Tour in Musketeer
- (U) Center for Math, Science and Technology Summer Camp Volunteering

(b) (3)-P.L. 86-36

Regular Features

- (U) KRYPTOS Contest winners:
  - Literature Awards
  - Tech Talk Awards
- (U//~~FOUO~~) Meet the Intern [redacted]

Editor's Desk

(U//~~FOUO~~) Welcome to the November 2002 edition of Tales of the Krypt. A major theme of this issue is the range of activities being done by cryptanalysts, from a renewed interest and focus on diagnosis ("Diagnosis: Concern and a Turning Point) to a plethora of more non-traditional areas where CA skills can help the mission (including [redacted] We also bring you an update on the CA new hires and the newly revamped CA curriculum, a list of KRYPTOS contest

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

(b) (3)-P.L. 86-36

[redacted]

winners, a CA intern interview (regular feature) and an article about and advertisement for volunteering to help out with the Center for Math, Science and Technology Summer Camp. - [redacted] *Editor TOTK*

(U) Diagnosis: Concern and a Turning Point

(b) (3)-P.L. 86-36

by [redacted]

(U) Prolog

(C) If you pay attention to the winds sweeping through the cryptanalysis community, you may have noticed a change recently. People are talking about diagnosis. Division chiefs, branch chiefs, technical advocates, and front-line analysts, all seem to have issues with the state of diagnosis. There was even a call into Talk-NSA with the Director asking his opinion of the current situation! What is going on here? What are the issues? Is diagnosis in trouble? As a branch chief of a diagnosis branch, I will try to give a balanced view of the discussions.

(U) What is Diagnosis?

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(S) Loosely speaking, diagnosis is the cryptanalytic discipline in which cipher, key, or cryptovariable generation schemes are recovered by scrutinizing the data alone. Diagnosis is arguably the hardest task a cryptanalyst is asked to do. It can be described as a circular process. [redacted]

[redacted]

[redacted]

(S) Finally, a diagnostician needs to have faith that the answer can be found and the desire to continue to search for it. A million tests have already failed. Other analysts have already poured over the data. Several diagnostic successes have occurred when other analysts have moved on to greener pastures leaving only a tenacious, faithful few to discover the answers.

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) History

[redacted]

~~(TS//SI)~~ [redacted]

[redacted] Many diagnosticians felt promotions to higher grades (14 and 15) were less than fair share. Further, CMP and AMP hires, who traditionally sought tours in diagnosis areas, tended to look elsewhere for work which would lead to the success and publications vital to their promotions. The CA program, though recently revitalized, was only producing one or two graduates a year, most without strong diagnostic skills. Finally, retirement claimed a number of excellent diagnosticians. Thus the number of skilled diagnosticians, especially modelers, dwindled.

(b) (1)
(b) (3)-P.L. 86-36

[redacted]

[redacted] (b)(3)-P.L. 86-36

were left to do their work. While the events of 9/11 brought some attention to diagnosis problems, the war against terrorism also made it even harder for Target Pursuit to give a long-term look at any issues not directly related to the immediate crisis.

(~~TS//SI~~)

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

Diagnosis is definitely not dead! But these successes cloud the critical juncture we have reached in building and maintaining a cryptanalytic workforce equipped to face future diagnostic challenges. Concerns about the technical health of the diagnosis community and the need to act soon to prevent the eventual extinction of the NSA diagnostician reached a head in May 2002.

(U//~~FOUO~~) The Draft and Forward

(b) (3)-P.L. 86-36

(U//~~FOUO~~) Technical Director for Data Acquisition, drafted a paper on the state of diagnosis which made its way to the larger community. This paper was supported by several CA technical leaders, who saw a need to increase participation in the future of diagnosis and were willing to take responsibility for it. The paper made the following assertions, some of which we have already alluded to:

(~~TS//SI~~) This paper has prompted a plethora of meetings, e-mails and discussions up and down the leadership chain. For example, in Data Acquisition's Strategy Implementation Plan (dated 24 June 2002), we find:

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

3.2.6 (U//~~FOUO~~) Encourage participation in diagnostic cryptanalysis by increasing promotions and awards in the same proportion as the CNE skill field.

(S) Within Target Pursuit, management at all levels generally agreed with the assertions made within the paper but there was much more disagreement about the appropriate solutions. The need to reorganize and create an office devoted to diagnosis was especially controversial. [redacted] the deputy chief of CES, met with the Target Pursuit division chiefs to discuss all of the issues and asked for a counter-proposal. He also met with diagnosticians in Target Pursuit to get their perspective. As a result of increased management focus on diagnosis, a number of initiatives have been started, including increased emphasis on teaming and sharing information across the target divisions, the reinvigoration of integrated diagnosis focus teams, and a new program of diagnostic fellows.

[redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(S) [redacted]

(U//~~FOUO~~) The surge in CA intern hiring is also providing an opportunity for diagnosis. The bumper crop of highly skilled and enthusiastic interns have filled many desks throughout the CA community. The movement of the program from the National Cryptologic School to S3T has the advantage that it now has its own promotion allocation, its own awards allocation, conference funding, and book purchases. This allows the intern program to address the problems pointed out in the [redacted] Draft on its own grassroots level.

(U) Final Thoughts

(b) (3)-P.L. 86-36

[redacted]

(b) (3)-P.L. 86-36

(U//FOUO) The [redacted] Draft called for major surgery and a long-term recovery program to return the diagnosis body to health. The OTP initiatives are certainly more than Band-Aids, but are they enough to ensure a thriving diagnostic future for CES? It depends on how healthy diagnosis really is and how strong our leaders commitment is to its future.

back to top

(U) CA Intern New Hire Update

by Linda Sutton

(U) For those of you who are interested in the latest demographics of the CA Interns, we have gathered that information with an emphasis on the last fiscal year new hires.

(b) (3)-P.L. 86-36

- (U) There are currently [redacted] interns, including [redacted] who joined the program within the last year. One of these [redacted] is technically not a new hire. This CA Intern previously worked here at NSA but joined the Interns as a "Cross Trainee".
- (U) Here are some demographics on the new intern class:
- (U) Females out number males two to one. There are [redacted] females and [redacted] males comprising the [redacted] CA interns coming on board in 2002.
- (U) [redacted] of the [redacted] are believed to have been hired into the CA Intern program as a result of the job fair in February 2001.
- (U) [redacted] were recruited directly from college and joined the NSA within a year of leaving college.
- (U) [redacted] of the [redacted] had advanced degrees at EOD.

(U) Educational backgrounds are varied but more diverse than you may think. The CA Interns have degrees in Mathematics, Physics, Computer Science, Computer Engineering, Finance, Business, Law, Criminal Justice, Astronomy, and Symbolic Systems. But the greatest number of degrees are of the Math and Computer categories.

(U) The award for the 2002 CA Intern hired from the greatest distance belongs to the Intern hired from Alaska. On the other hand approximately [redacted] are from the Virginia / Maryland area. Four were hired from Ohio, and two from both New York and Texas. Other hirees EOD'd from Illinois, Massachusetts, Michigan, Minnesota, Mississippi, New Jersey, Nevada, Pennsylvania, South Carolina, and Vermont. And though the 2002 Interns were hired from these states, several interns profess to origionally be from other locations.

(U) Initially hiring projections for 2001 were set at [redacted] were hired. For 2002 the initial figure was to have been [redacted] were hired. For fiscal year 2003, again [redacted] have been hired to date.

back to top

(b)(3)-P.L. 86-36

(U) CA Curriculum Review

[redacted]

by [redacted] (b)(3)-P.L. 86-36

(U//~~FOUO~~) In April 2001, the Signals Analysis, Cryptanalysis and Math Office (then E5) of the National Cryptologic School, the Cryptanalysis Skill Community and SIGINT Directorate (SID) conducted an audit of the Cryptanalysis curriculum. The purpose of this audit was to determinetraining gaps and assign action items to ensure that the curriculum would consider current and future training needs. The two day audit identified several issues that needed to be addressed in restructuring the curriculum:

- delivery of existing courses
- outdated intern program training
- lack of courses for the mid-level analyst, especially on modern communications and emerging technologies
- need to create training that does not rely as heavily on platform instruction
- need to build a stronger partnership between NCS and the CA community.

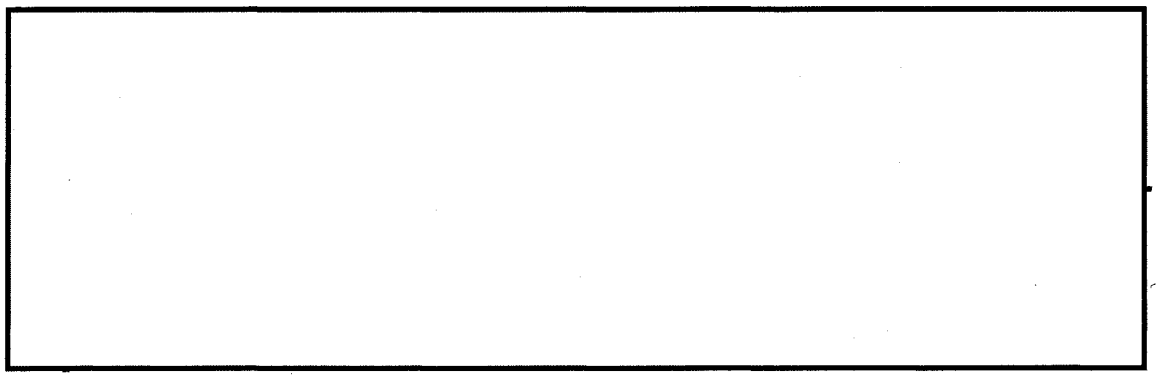
(b)(3)-P.L. 86-36

(U//~~FOUO~~) A post-audit curriculum study group was formed just prior to September 11 to survey the skill community for additional recommendations. As a result of the post-crisis activities, most of the volunteer members were unable to help in the short term but, in late November a small group of volunteers were able to go forward with the interview process. Interviews were held with [redacted] people in SID and IAD in December 2001 and January 2002. The list of interviewees included deputy division chiefs, branch chiefs, technical advisers, interns, and adjunct instructors, as well as the chiefs of CES and OTP.

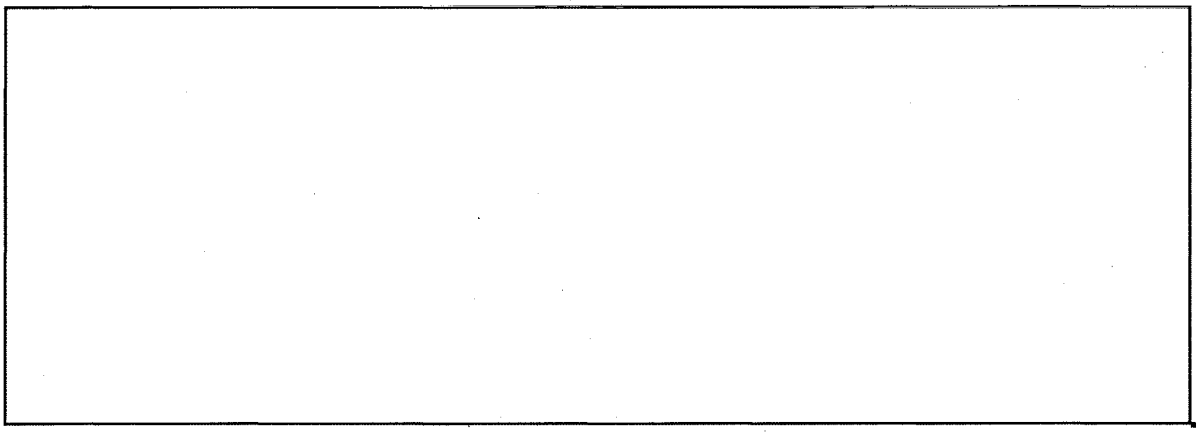
[redacted]

(b)(1)
(b)(3)-P.L. 86-36

[redacted] (b)(3)-P.L. 86-36



(b) (3)-P.L. 86-36



(b) (1)
(b) (3)-P.L. 86-36

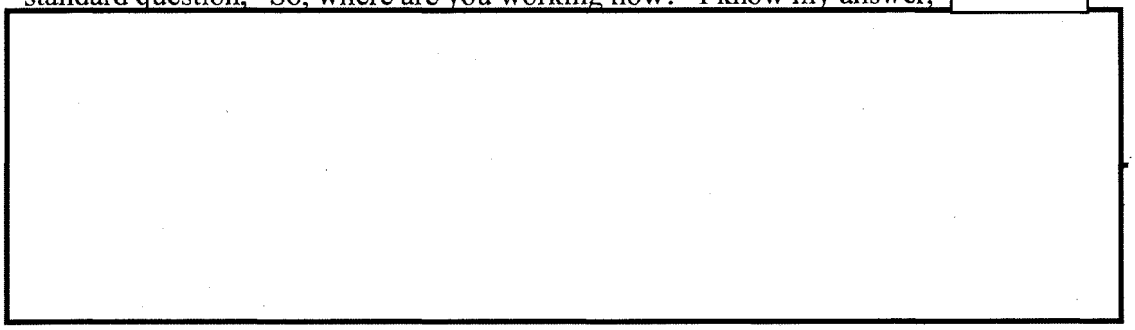
back to top

(U//~~FOUO~~) A Cryppie's View from [redacted]

(b) (3)-P.L. 86-36

by [redacted]

(~~S//SI~~) When I come across someone I haven't seen for a while, I sheepishly await the standard question, "So, where are you working now?" I know my answer, "[redacted]



(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) I'm not surprised by the lack of familiarity with [redacted] The demanding pace of our jobs requires us to be judicious in what we allow to appear on our radar screens. Understandably, many of us have become numb to the promise of the next fix-all initiative. I also understand the ribbing retort of, "When are you going to return to real work?" Most of my peers would never choose a full time job primarily consisting of meetings, phone calls and documenting, even if the goals were laudable. I knew [redacted] mission would be a landmine of frustrating challenges, and I had already

(b) (3)-P.L. 86-36

[redacted]

beaten my head against many brick walls during other initiatives. But when I was asked about joining [redacted] I recognized that the backing of the SID Director provided the authority and scope for making a significant difference.

(U//~~FOUO~~) My choosing to work in non-traditional CA roles implicitly suggests that I think the CA/Math community has something important to contribute. I'm proud to be part of this community comprised of creative, technically adept problem solvers who can tackle the open-ended and ill defined. The power of this community's technical might is awe inspiring, but cannot realize its full potential functioning in isolation. The success of what each of us does is dependent on what comes before and after us; we all have the responsibility to understand how what we do fits into the end-to-end SIGINT process. I take this very seriously and want to help remedy systemic problems which inefficiently use our brain trust and impede our overall effectiveness.

(U//~~FOUO~~) I accepted a long time ago that you cannot always assume that every relevant problem has an advocate who is seeking its resolution. We're all just a bunch of human beings doing our best, and no one person can expect to have all the answers or the grand plan. I do see opportunities for improvement, though. Therefore, when something seems amiss I'm going to try to find out if a plan exists to improve the situation. If not, then my annoying fix-me response gets into gear. (I grew up with a hyper sense of responsibility, accountability, and an inability to say no - hence my consenting to write this article! Fortunately this is all tempered with my love of things outside of work.) Armed with 14 years of technical experience, an innate desire to want to help and a naivete to think that I can, I signed on for 18 months of [redacted] (Not sure about the option to renew.)

(b)(3)-P.L. 86-36

(~~S//SI~~) It's been a challenging, interesting and worthwhile experience thus far. I've enjoyed the construct of small teams comprised of individuals from across SID working together to affect real change. Of the two of us originally tasked to lead the effort against [redacted] I was anointed the Data Acquisition (DA) "expert." This presented me with an opportunity to make unique and valuable contributions while also being stretched to learn more about DA and other less-familiar areas of the Intelligence Community. (At least I can now claim greater competency in understanding SID's organizational structure!) With a mission to act as a catalyst for change and foster the development of new and innovative strategies we were empowered to go off and do good things. Such a huge mission with so many possibilities for proceeding required creativity, risk taking, perseverance, a holistic approach to tackling the target, and a plan. By design our smallness necessitated a greater dependence on leveraging the resources of the extended enterprise. In less than 12-month's time I've worked with CRD and every Group-level

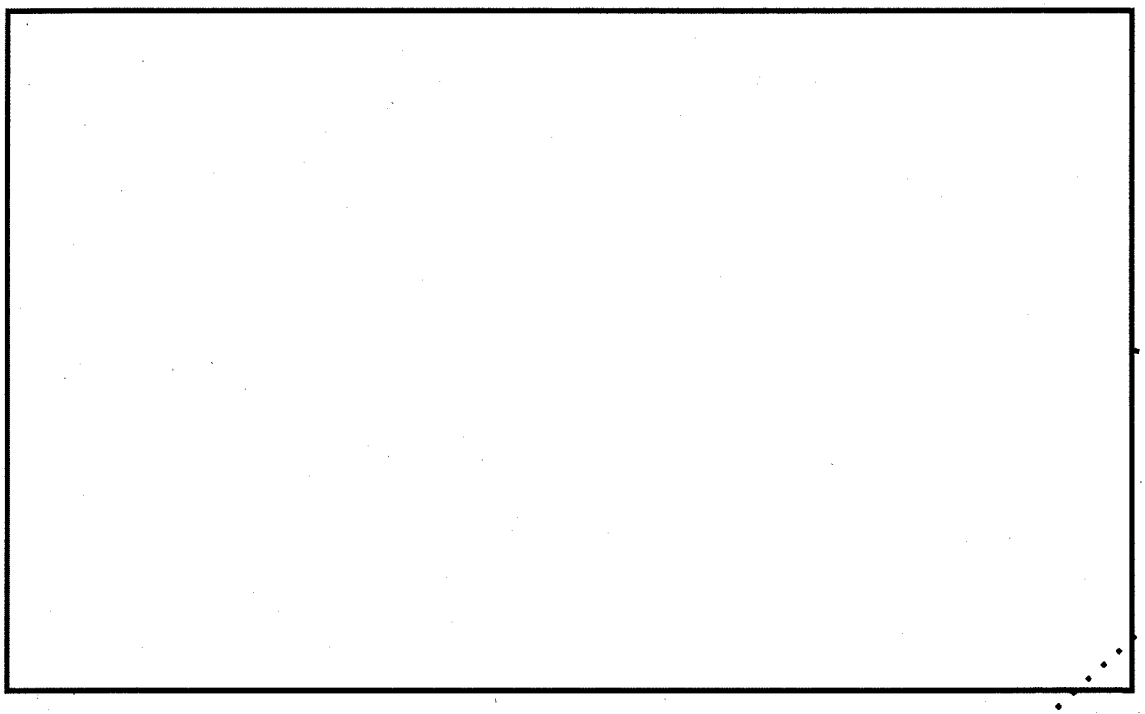
(b)(1)
(b)(3)-P.L. 86-36

[redacted] as

[redacted]

[redacted]

(b)(3)-P.L. 86-36

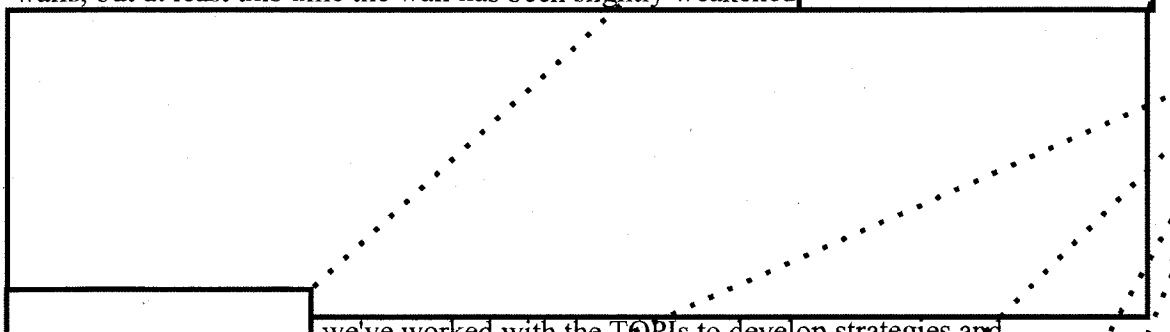


(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//SI)~~ The cool thing is that all of the task forces can claim success to one degree or another. Of course, we didn't fully achieve the lofty goals we wish we could have, but there has been real progress. Offices are now utilizing collection vehicles and techniques that were unfamiliar to them [redacted] and which are now providing them access to additional desirable intelligence. There is better collaboration between NSA and its external customers and partners (e.g. CIA, FBI, the Commands). Not surprisingly we received overwhelming feedback that one of the biggest benefits of [redacted] was in bringing people together and raising the awareness of everyone involved.

(b) (3)-P.L. 86-36

~~(S//SI)~~ For me much of what I anticipated came to fruition - lots of head meeting brick walls, but at least this time the wall has been slightly weakened [redacted]



[redacted] we've worked with the TOPIs to develop strategies and transition plans to help them build upon the progress already made during [redacted] first iteration.

~~(S//SI)~~ I was asked to write an article about a CA in [redacted] but I believe the bigger issue is how we, as members of a core discipline, see ourselves as part of the bigger SIGINT community. One of the heartening aspects of working in [redacted] is being surrounded by people who see themselves as professional SIGINTers, who will give it their all to try to make the system work better. Sometimes we are vilified for interfering, but from where I sit, to a person, we are here because we care about the

state of SIGINT and we want to help. [redacted] is a reminder that: the simple approaches can make a difference, persistence pays and everyone has something to contribute. As confirmed by my experiences in nontraditional roles, the CA/Math community contributes not only a body of knowledge, but also a unique ability to solve problems and positively affect the future of this Agency.

back to top

(b)(3)-P.L. 86-36

(U//~~FOUO~~) [redacted]

by [redacted]

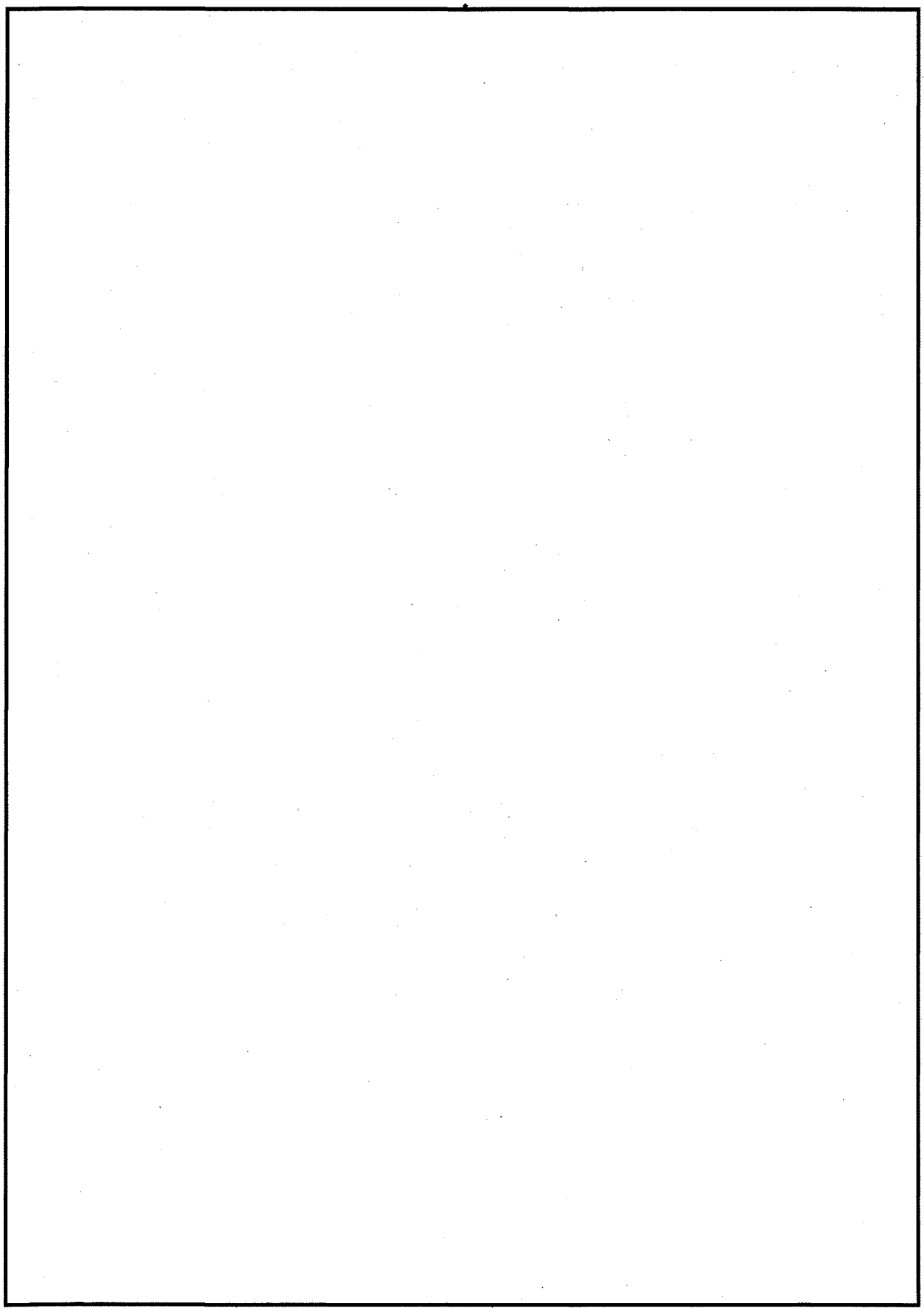
(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

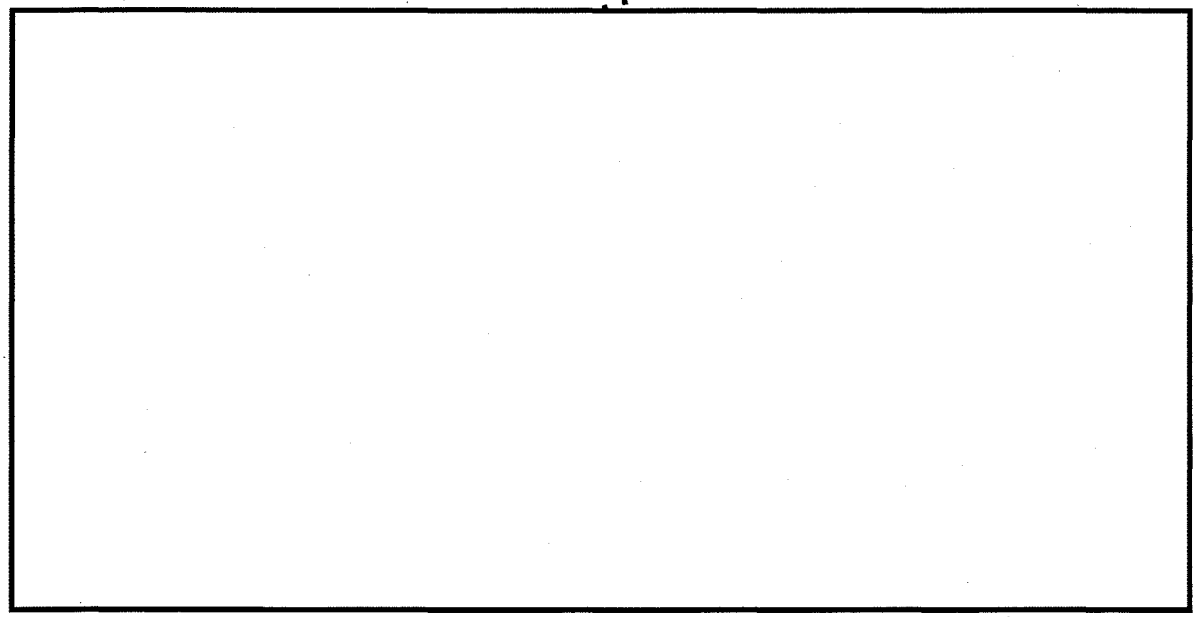
[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



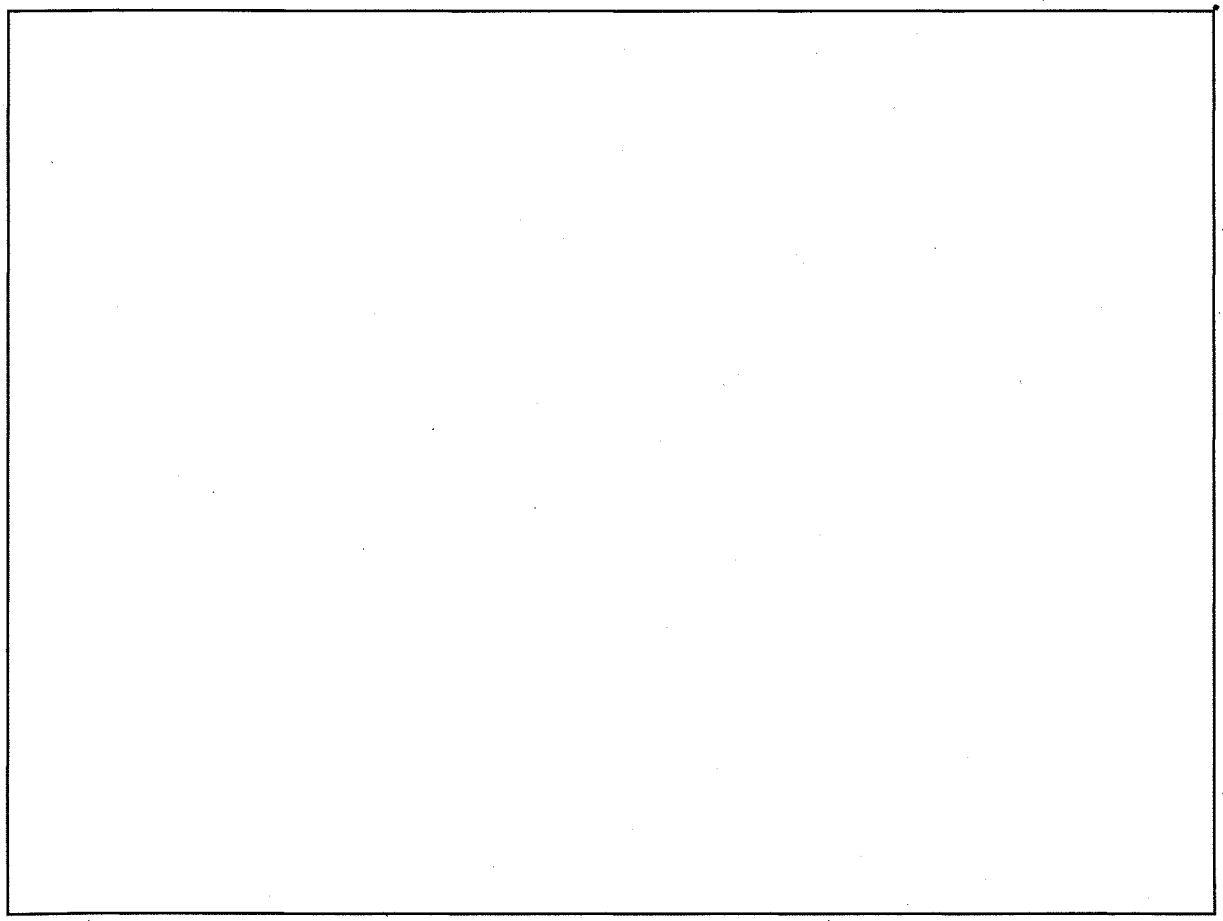
back to top

(U//~~FOUO~~)

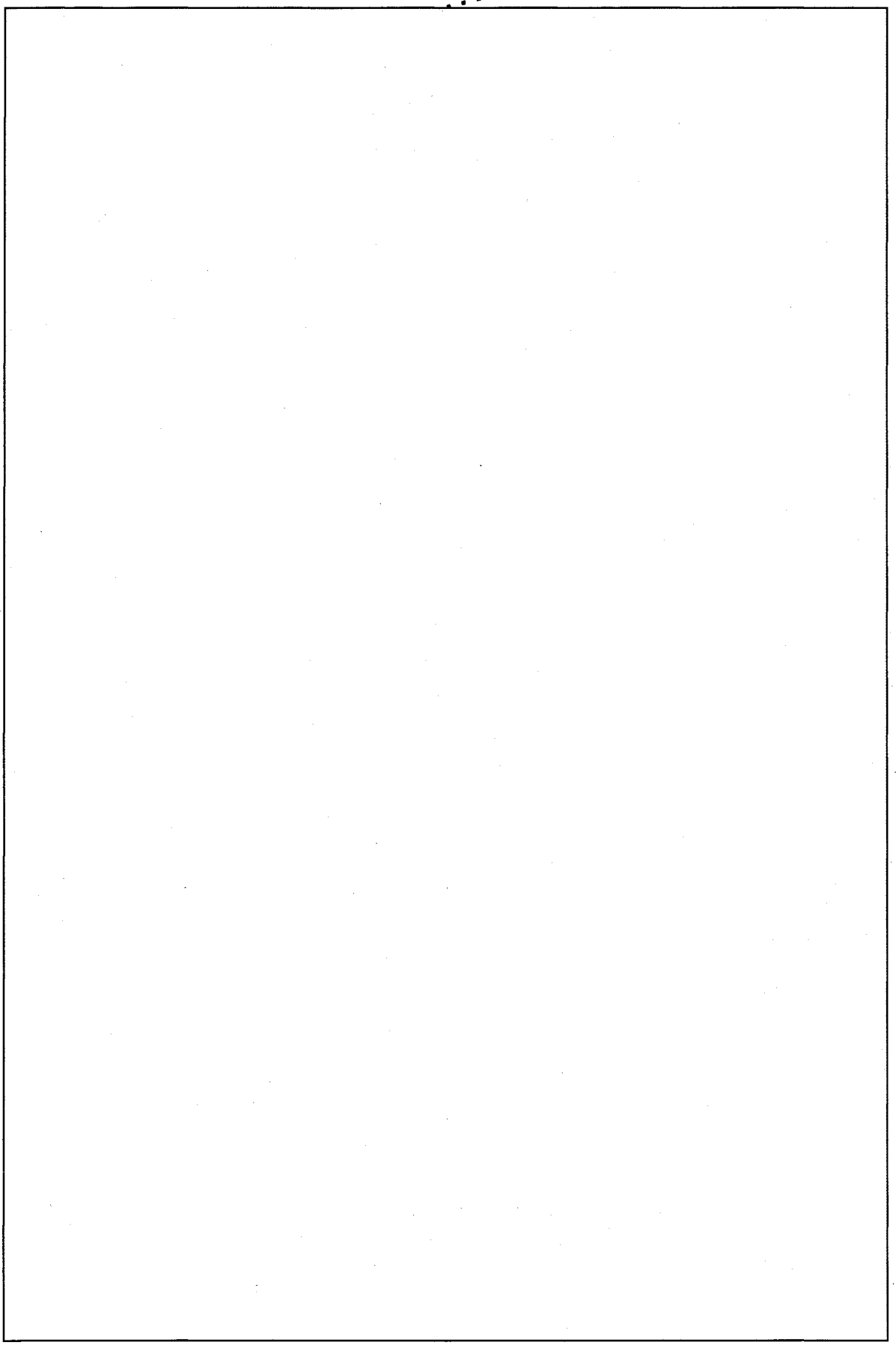
(b)(1)
(b)(3)-P.L. 86-36

by

(b)(3)-P.L. 86-36



(b)(3)-P.L. 86-36



thing is the mission and the people. That is what Chuck thinks is the secret to success as a manager: setting the right work environment for smart people to be creative and productive.

back to top

(U//~~FOUO~~) F6 as an Intern

(b)(3)-P.L. 86-36

by

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[redacted]

[redacted]

back to top

(U//~~FOUO~~) My Tour in Musketeer

(b) (1)
(b) (3)-P.L. 86-36

by [redacted]

(b) (3)-P.L. 86-36

(U//~~FOUO~~) I have been fortunate to be the first ever cryptanalysis intern in MUSKETEER. I am told it is not a typical CA tour, although I've yet to participate in a "typical CA tour." [redacted]

[redacted] The office is managed well, and the people with whom I worked, as well as those that I did not, are top-notch.

(U//~~FOUO~~) Because of my varied background in [redacted] I felt that MUSKETEER would be a good experience, and it has been.

(U//~~FOUO~~) I have worked on mostly SRTD work: Signals Research and Target Development, which is IA (Intelligence Analyst) work. I have been privileged to work with a brilliant senior analyst who is adept at mentoring interns. In his previous experience, the interns have been CMPers. So, this was a new experience for him as well.

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

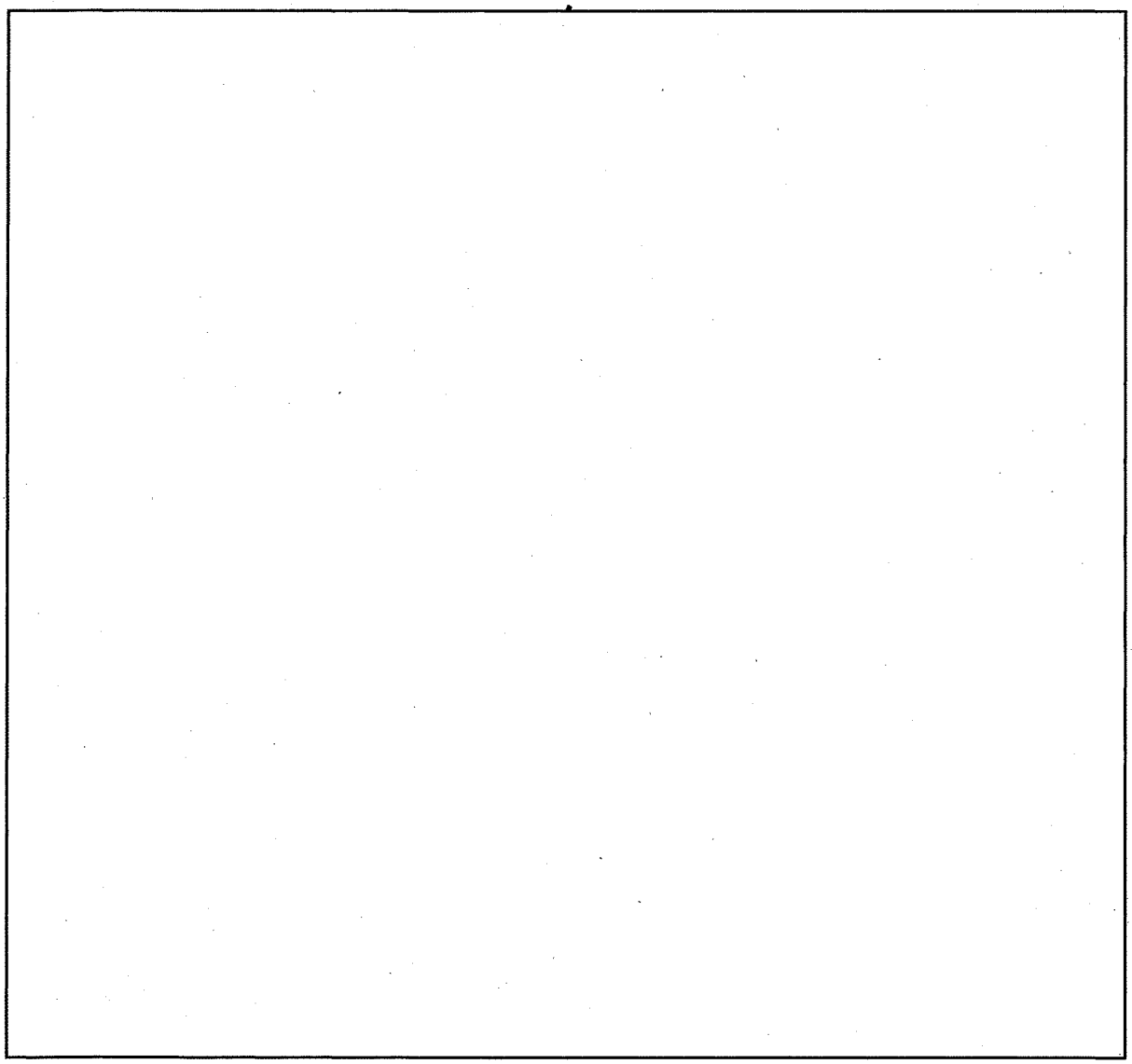
(U//~~FOUO~~) So, what has occupied my time when I am not in classes?

[redacted]

(b) (3)-P.L. 86-36

[redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36



back to top

(U) Center for Math, Science and Technology Summer Camp Volunteering

by [redacted] (b) (3)-P.L. 86-36

(U) When was the last time you built your own computer? How about gone surf fishing in the Atlantic off Assateague Island on the eastern shore? Or maybe played Pi-Chess? Or have you ever designed a home, built a model, created a blue print, and ended with a virtual tour of that home? Or have you considered the medical problems of launching people into space?

(U) These are a few of the adventures that NSA volunteers shared through the MEPP experience at either the high school or middle school sessions of CMST camp at the University of Maryland Eastern Shore.

(b) (3)-P.L. 86-36

[redacted]

(U) What is MEPP?

(U) What is CMST?

(b) (3)-P.L. 86-36

(U) Just type "GO MEPP" in the URL of Netscape. Many of you know of the wonderful opportunities with The Mathematics Education Partnership Program already. I, as a new CA Intern, made the discovery back in February when [redacted] sent the following email.

> (U) "The MEPP office is once again looking for volunteers to work at the Maryland Summer Center for Mathematics, Science, and Technology (CMST). CMST is a summer camp for gifted high school and middle school students and is supported in part by Agency funds. In addition to providing funds, the Agency also provides employees who assist with the teaching of various classes.
>
> (U) There are two sessions of camp each summer. Students select one class to take for the entire 2-week session. Each weekday, they attend that class for 3 hours in the morning and 2 hours in the afternoon.
>
> (U) Another hour of each day is spent in a secondary, non-technical class. The rest of the day is filled with recreational activities and special programs. On the weekends, students take a trip to a local state park here they swim, canoe, bike, and picnic.
>
> (U) For the last few years, the camp has been held at the University of Maryland on the Eastern Shore in Princess Anne, Maryland. It takes approximately 2.5 hours to drive there from NSA and is only 45 minutes from Ocean City. Princess Anne is a small and very old town with several historical sites.
>
> (U) Part of the CMST funds provided by the Agency is used to hire teachers to teach the classes. In addition to donating funds, the Agency provides volunteers to help out with the program. These employees spend two weeks working at CMST instead of at Fort Meade. Employees must get their supervisor's approval to volunteer at CMST.
>
> (U) Typically NSA volunteers assist the teachers with their classes. In some cases, volunteers team-teach with teachers. NSA employees are required to spend 5 hours a day in the classroom. Participation in the elective classes, the recreational activities, and the special programs is optional.
>
> (U) While at CMST, students live in the school dorms. When they are not in the main class, they are under the supervision of counselors who are usually college students. Teachers and NSA employees also stay in the school dorms but they do not live with the students.
>
> (U) In the past the program was open only to Maryland students. In recent years, however, this restriction has been removed and the program is now open to students from other states as well. Students must submit an

(b) (3)-P.L. 86-36

[redacted]

application, which consists of a record of their grades, letters of recommendation, and an essay. Those students who are selected are highly motivated and enthusiastic about being there. Teaching them is very satisfying.

(U) We are looking for volunteers who are enthusiastic about math and science, are energetic, and like working with kids."

(U) Consider volunteering for CMST next summer. The personal rewards abound. But there are a few other things you may want to know before making the trek.

(U) Yes, you live in a dorm. They are nice on the continuum of dorm ratings. Rooms are a good size with either single or double accommodations. Rooms are air-conditioned most of the time, and the beds . . . well, let's say that the beds are typical dorm beds. The mattresses are an 8-inch, vinyl covered, foam pad. Bedsprings are stretched across wooden frames. Be prepared should you have back trouble. In fact a few experienced individuals brought their own beds. Perhaps it's best to consider it a camping adventure.

(U) Heat and humidity was a problem for all camp participants. Some classes spend a great deal of time outdoors or on field trips. Also the extreme heat forced roaming brownouts during peak electrical usage hours when the school expects less occupancy. So it's important to bring your own fan because dorms took hours to cool back down.

(U) You eat in the University cafeteria. You can choose to dine with the students or other teachers. But remember cafeteria food at your college? Then you know the menus. They did have a twist to breakfast that was foreign to me. It was "scrapple". Apparently scrapple has a wide following and even has an entry in the dictionary. I thought scrapple was similar to fried Spam. But if you would rather eat cafeteria food than cook, it's great. It can be a vacation from your kitchen.

(U) You teach, or assist, in a class with an assigned lead teacher or two. Main courses are morning and afternoon, 5 days a week. While some volunteers were only there for one week because of mission, most of us stayed for both weeks. Volunteers are from many backgrounds, programs, personalities, professions, and so are the teachers. Some teachers were "nerds" and some were "partiers". Just like the rest of the world. Yet volunteering with CMST this does offer a time to network, regroup, and make friends unlike any other.

(U) An area that I was not prepared for was the "elective" class. Teachers and volunteers were encouraged to create four one-hour activities for the students. I was lucky. Two teachers needed assistance in an elective that required one adult for every three students. I became part of the elective "Gone Fishing". That's exactly what we did. Each day at 13:00, we escorted 9 students on a 1-hour fishing trip to several of the streams on and off campus. You can imagine how difficult the assignment was.

(U) All joking aside, many of the student's had never fished before. The excitement of pulling in their first Sun Perch or Croaker or Crab was priceless! (Not to mention watching students bait the hook with a worm for the first time.) It would be great to know how the students described the experience to their friends and families.

(b)(3)-P.L. 86-36

9/24/2010

(U) Volunteers experience variations in their feelings of value to the class experience. My particular class was "Bay Rangers", a biology based middle school course about the Chesapeake Bay. I assisted two regular middle school teachers who were not math people but one science and one a social studies teacher. It was quickly obvious that my contribution would be to make the "math" connection to the sciences. For example, I explained the logarithm pH scale with visual demonstrations. I taught the kids to used simple geometry and trig to estimate volumes and surfacc areas of bodies of water. And when the students wanted to measure the flow rate of one of the streams at the University, I provided the basic formulas. The students gained a sense of how important math is to the biological sciences.

(U) The Bay Ranger class involves several field trips. We toured an electric power plant, a Chesapeake research center, seined for fish, collected water samples, went crabbing, tromped through wetlands, walked through an automated pig farm, and held our noses through a sewer treatment plant. All these activities are inter-connected with the Chesapeake. In other words we had some smelly experiences. The students rarely complained and wanted to know if they could sign-up for the class again next summer.

(U) Here is a list of the classes taught during both the high school and middle school sessions:

Middle School Session - July 13-27, 2002:

Mathematical Mind

Aeronautics and Rocketry

Codes, Games, and Chance

Astronomy Village

Bay Rangers

Programmatics

Mathematics and Architecture

High School Session - June 22-July 6, 2002

Fractal Geometry & Chaos

Advanced Problem Solving

Technomatics: Linking Programmable Technology and Mathematics

Life on the Bay

All the World's a Physics Toy: Flights of Fancy with Physics

High Confidence Software Design Techniques and Tools

(b)(3)-P.L. 86-36

Mathematics and Chemistry/Chemistry and Mathematics

Space Medicine Research and Technology

Classical Cryptanalysis: The Science of Code breaking

Digital Logic

(U) As you can see, there were topics for all interests. Students submitted class preference lists with initial applications. In most cases first or second choices were granted. Initially a few students grumbled about their assignment but by the second week of camp, students seemed content with their placement. For the most part students who did not receive initial choices had enrolmented late.

(U) The very best parts of the camp are the students. They are amazing. The young people you meet at CMST **want** to learn! They were supportive of one another, cooperative, well behaved, energetic, and eager to learn. Many of the students are gifted and sometimes lack peer groups in their regular school environment. This camp provides an environment of acceptance and encouragement for all students.

(U) CMST is a great adventure, especially if you like working with young people. Consider volunteering next summer.

back to top

(U) KRYPTOS Literature Awards

(b) (1)
(b) (3)-P.L. 86-36

- **First:**
- **Second:** (U//~~FOUO~~) BioMetrices by BioLink by
- **Third:**
- Honorable Mention: (U//~~FOUO~~) SecuGen: Thumb Thing to Remember Me By by

Special thanks and appreciation to this year's literature contest judges:

back to top

(U) KRYPTOS Tech Talk Awards

(b) (3)-P.L. 86-36

- **First:**
- **Second:**
- **Third** (tie):
  (U//~~FOUO~~)

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) The German Enigma - It's Origins, Evolution, Exploitation by

back to top

(U) Meet the Intern -

(b) (3)-P.L. 86-36

by

(U) Editor's Note: After interviewing Tim a number of months ago, the author lost her notes and had to recreate the information from memory. Tim supplied some of the missing information, so this article is both an interview and an autobiography.

(U//~~FOUO~~) is a CA intern who is willing to stand up in a crowd - perhaps you noticed him cheering for

is enjoying the challenges of cryptanalysis. He likes working with smart people on hard problems and he was pleasantly surprised to learn he enjoys programming, which is something he largely stayed away from in school. Yet he still has plans to one day return to teaching at

(b) (6)

(U//~~FOUO~~) It is almost a cliché in our community that there is a positive relationship between interest in music and talent for cryptanalysis. This would explain why being a lousy musician, also stinks at Cryptanalysis. (wrote the previous sentence himeself; the editor notes it is inaccurate.)

(b) (3)-P.L. 86-36

Meet the Intern *is, hopefully, a regular feature of TOTK. Individuals are encouraged to interview Cryptanalysis interns and send contributions to for publication in this forum. This feature is meant to be informative and light, if not outright funny... never degrading.*

back to top

DERIVED FROM: NSA/CSS MANUAL 123-2
DATED: 24 FEB 1998
DECLASSIFY ON: X1

~~TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, AND NZL//X1~~

(b) (3)-P.L. 86-36

~~TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, AND NZL//X1~~

(S) POC:

(U)CES EXTERNAL PAGE

Tales of the Krypt - July 2003

Feature Articles

- (U) Words of Wisdom Regarding Cryptanalytic Software
- (U) Meandering with : The View From My Piroque
- (U) Unique And Unusual Encouters for a New Cryptanalysis Intern
- (U) CA: Then and Now

Regular Features

- (U) Awards: Gold Bug Team Award
- (U//~~FOUO~~) Meet the Intern

(b) (3)-P.L. 86-36

(U) Words of Wisdom Regarding Crypanalytic Software

by

(b) (3)-P.L. 86-36
(b) (6)

(U) Editor's Note. Since our readership enjoys the articles on Meet the Intern, the authors of this article felt a similar emphasis needed to be placed on capturing words of wisdom from retirees. They have proposed a continuing series called "Meet the Retiree".

(S//SI) and recalls her first days at the Agency as "not knowing anything". She was given some conference papers to read and she says they might as well have been in Greek since she didn't understand any of it. She was also confused by all the covernames and acronyms. She was handed an IMP manual and had to learn this in-house programming language and the on her own. "Isn't it funny how some things do not change over the years?" Many of the new hires today have the same feelings that did back then. Luckily, many interns now have mentors and "buddies" to help them.

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

Approved for Release by NSA on 09-28-2023, FOIA Case # 61704

(b) (3)-P.L. 86-36

(S//SI) One of [redacted] words of advise is that the CA community (especially Target Pursuit) needs to take a stand, get actively involved and demand support for cryptanalytic software packages. She feels that the CA community currently has a passive role in software packages. That is, if you ask a question you will get an answer. Someone or several someones are needed who will pound loud and demand that our needs are heard and met. She wants us to remember that the analytical tools are customer driven. If there are no customers driving, then nothing gets done. However, she also realizes that it is difficult to drive today because there are many steps to the requirements process. But it is doable. [redacted] points out that there is a champion who strongly supports the Signals Analysis software efforts and that the math community is supporting [redacted] When asked whether

(b) (1)
(b) (3)-P.L. 86-36

[redacted]

(C//SI) [redacted] believes in the quote "You can give a man a fish and feed him for a day or teach a man to fish and feed him for life." [redacted] practiced that principle by passing along bit-level programming skills to anyone who asked. She especially loved the customer support part of the job and would often help people who were having trouble with their code. She feels that CA interns with a computer science speciality should be allowed and encouraged to work in her branch.

[redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U//FOUO) [redacted] worked on [redacted] for 15 years. She is referred to as **THE [redacted] Queen** because she took on many important leadership and librarian roles in addition to programming. She is highly regarded as the "*mom*" of the team and many cryptanalysts and mathematicians respect and value her work and judgement. To this day, when analysts talk about the [redacted] programmers they envision a giant team of programmers because it is such a well developed and well maintained package. But in reality, there are [redacted] members of the team. With the retirement of [redacted] a huge gaping hole will be created. Even though there aren't many people who can fill [redacted] hoes, the fact that no one will be allowed to try is a shame.

(b) (3)-P.L. 86-36

back to top

(U) Meandering with [redacted]: The View from my Piroque (1).

by [redacted]

(U) Introduction

[redacted]

(b) (3)-P.L. 86-36

[redacted]

[redacted]

(U//~~FOUO~~) What is [redacted]?

[redacted]

(U//~~FOUO~~) Although the article can be read without them, [redacted] commands that go along with the text are included. For those used to reading math books with pencil and paper nearby, this should seem natural. Interested readers can start a new xterm and from C-shell type

[redacted]

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) Capabilities

(~~TS//SI~~) Here are some [redacted] features I've found useful.

[redacted]

[redacted]

[redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted]

(U//~~FOUO~~) 1, 2, 3, 4, ... (b) (3)-P.L. 86-36

(~~TS//SI~~) Counting is often one of the first steps in diagnosis, frequently followed by a [redacted] here are example files in the [redacted] documentation that show how to do basic counts.

(U//~~FOUO~~) Editor's Note: Unfortunately, some material had to be excised from this article because of classification concerns. We hope that future editions of this magazine, including the full version of this article, will be hosted in a [redacted]-friendly, web-friendly environment.

(b) (1)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) Interoperability

[redacted]

(U//~~FOUO~~) Recent Personal Experiences

[redacted]

(U//~~FOUO~~) Visualization

[redacted]

(U//~~FOUO~~) Learning Curve

(~~TS//SI~~) There are always bumps in the road to knowledge of a new computer language. Developers make choices that may not be intuitive for a novice user or best suited for a user's intended application. I certainly had my share of frustrations. As a new user it took some time to become accustomed to the jargon and the format of the [redacted] unabridged reference. With experience, learning from the documentation has become much easier, but searching is not a picnic. A [redacted] would help tremendously (note(2)) . It helps to work together with colleagues, especially at the beginning.

(U//~~FOUO~~) Why [redacted]

(~~TS//SI~~) Doing diagnosis means performing lots of mathematical experiments and tests, some of which need to be tailored to the particular data being investigated. Usually I'm more concerned with optimizing development time than minimizing CPU cycles. The calculus regarding time-efficiency in the medium term indicated that for me - despite the learning curve - [redacted] is an effective way to perform many CA tasks. As I've become more comfortable with the terminology and capabilities of [redacted], programming has become easier and faster than doing the

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

[redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) Acknowledgements

(~~S~~) Thanks to [redacted] and several others from the [redacted] Diagnosis Focus Team and to the editor for their helpful suggestions.

(U//~~FOUO~~) (1) piroque: a small boat similar to a canoe oft used in the marshes of southern Louisiana, see any Cajun-English dictionary. (top of article)
(~~TS//SI~~) (2) Apparently in response to the remark above, there is (on 7/16/2003) a [redacted] (back)
(U//~~FOUO~~) (3) SLUG: a member of the Scripting Languages Users Group (back)

back to top

back to top

(b) (3)-P.L. 86-36

(U) Unique and Unusual Encounters for a New Cryptanalysis Intern

by [redacted]

(U//~~FOUO~~) [redacted] and I entered on duty to the NSA as cryptanalysis interns in July of 2002. Fortunately for us, we were given the opportunity to experience CA intern limbo until our first class was scheduled to begin a few weeks later. We participated in online classes, completed some bypass exams, and learned about the inner workings of the National Security Agency. Consequently, [redacted] took to the phones and tried to organize for us any tour of any government establishment, NSA related or not, that he could conceivably wrap his brain around. You name it: he contacted the White House, the Pentagon, the FBI, the CIA, the Director of the NSA, and many others. And by contacted, I do mean he actually spoke to people, not just computers and machines. When he spoke to the person at the White House, she actually asked him what the NSA was. At first, he had limited success, but eventually his diligent efforts paid off. He landed us lunch with the DirNSA, Gen. Hayden, and a tour at the CIA. Immediately we were ecstatic. I, for one, did not harbor any previous thoughts that the DirNSA would actually have lunch with an everyday-employee let alone three recently inaugurated interns. We had heard that he would eat lunch sometimes in the cafeteria, amongst us "common folk", but to a new NSAer, what was accomplished seemed to be a coup.

(U) We were invited to a brown bag lunch to be held at the director's office with some other new hires. I, being the eternal "optimist", figured we were going to be among fifty or a hundred other interns and the director would only pop in to say "hi." I was not going to pass up this opportunity, however, especially considering it was either have lunch with the director or stay in the pleasant little classroom at FANX all by my little self. Fortunately for us, my optimism radar was way off and lunch turned out to be more intimate than I expected. In all, there were nine in attendance: the three of us, the Director, his secretary, some direct hires, and a recent military assignee.

(U) General Hayden's office is modest, as expected by the importance the Agency puts into ambience, but still has some personality, including a display of memorabilia of the Pittsburgh Steelers. As probably should have been expected, the director came prepared. He had bios on each of us, which included college transcripts complete with highlighted markings. He asked all of us questions about our recent employ and how we were fitting in to the Agency and seemed to be genuinely interested in our responses. He talked to us about how he views the role of the NSA in the modern world, the importance of helping the citizens of the United States to have a better understanding of what we do, and his concerns for the future. He also talked to us about September 11, 2001 and how the Agency was affected. There was not a single dull moment at lunch. It lasted about an hour and ended with the feeling that we had just been to the moon.

(~~S~~) A couple of months later came the tour of the CIA [redacted] shmoosed again and it turned into an all day outing for nearly half of the current CA interns, plus [redacted] We took the blue bus to Langley and, upon arrival, we were given a tour of the memorials on display in the foyer of the headquarters building. The "Memorial Stars" display honors CIA officers who lost their lives while in service to the Agency and the Office of Strategic Services Memorial honors officers of CIA's predecessor organization (OSS) who lost their lives during World War II. Then, we were ushered to an auditorium to begin a series of briefings. These were given by CIA and

(b) (3)-P.L. 86-36

[redacted]

[redacted] Next spoke a CIA agent of many years who basically solicited a plea for us to continue sharing information with each other. I got the impression that he had some experiences, not necessarily recent, that suggested otherwise. Then came CIA's version of "Q" from the James Bond adventures (we'll call this a Zest moment, not because the speeches were in any way uninteresting, but simply because it was Q). [redacted] I could tell you more, but then ... we'll leave it at that.

(b) (3)-50 USC 3024 National Security Act of 1947 Section 102A(i)(1) CIA 3.5(c) Section 6 of the Central Intelligence Agency Act of 1949, 50 U.S.C. 3507 OGA

CIA

(U) A tour of CIA's exhibit center followed. The museum is maintained by CIA's Center for the Study of Intelligence (CSI) and contains collections of historical intelligence artifacts. We had the opportunity to examine personal memorabilia from Major General William J. Donovan, the founder of OSS and from collector and historian H. Keith Melton. The display includes many clandestine espionage memorabilia and is currently the world's largest collection of spy gear. My favorite part of the collection was a rock from President Bush's ranch in Texas. And really it was just a rock. Following the walk through the CSI museum, the tour ended with the opportunity to view a section of the Berlin Wall memorialized at the CIA, viewing some model spy planes donated by Lockheed Martin, the infamous "Kryptos" sculpture designed by James Sanborn, and the gift shop, which happens to be much more expensive than the gift shop here at the NSA.

(U) After experiencing these two events, being a new intern did not seem so bad and as [redacted] put it, "We felt very welcomed into the intelligence community." He went on to say, and I am sure others will agree, that being able to set up these opportunities made the sky the limit. Of course, taking those first steps are the key.

back to top

(b) (3)-P.L. 86-36

(U) CA: Then and Now

by [redacted]

(S) When [redacted] began their careers at NSA in the late sixties, cipher traffic came typed on onion skin paper with multiple carbon copies, computers were about to be the next big thing, and nobody wore jeans to work. After being classmates at a local high school, [redacted] met again while working as cryptanalysts in the [redacted] did two years of unrelated military service first. Fittingly, they are now back together, rounding off their respective careers in the Target Pursuit branch responsible for [redacted] To get a feeling for how the daily life of a cryptanalyst has changed, TOTK recently interviewed [redacted] about their experiences.

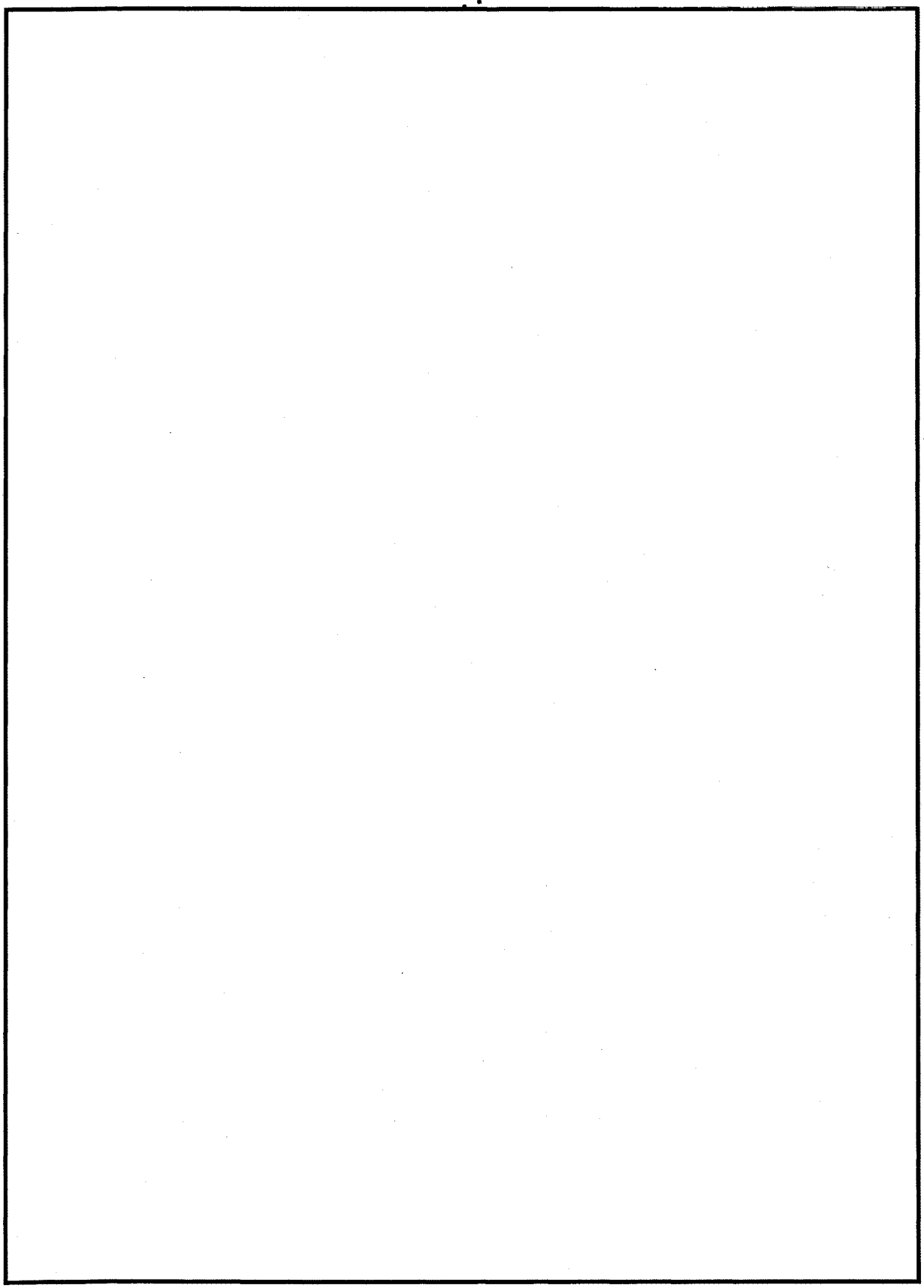
(S//SI) [redacted] was initially assigned to the typing pool, which was made up of all women (referred to as "girls" according to the culture of the times), often recruited from the commercial curriculum of local high schools. The typists punched the cipher messages onto 7-level paper tapes, so that the cipher could eventually be fed through analog machines designed by the Research & Development organization to automate the decryption process. In time, of course, the preparation of messages was also automated, although today's cryptanalysts do still sometimes find themselves manually entering cipher, perhaps from a handwritten fax or transcribed from a voice communication.

(S//SI) Punching the paper tapes was painstaking work: if you made a mistake, you had to use correction tape and a special machine to cover the mis-punched holes and repunch the correct holes. Even though they were not given special training, [redacted] found that she quickly learned the relationship between the letters and the punch patterns, almost like learning a new alphabet. This was important since the letters themselves did not appear on the tapes - only the hole patterns. Typical messages were [redacted] There were two

[redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

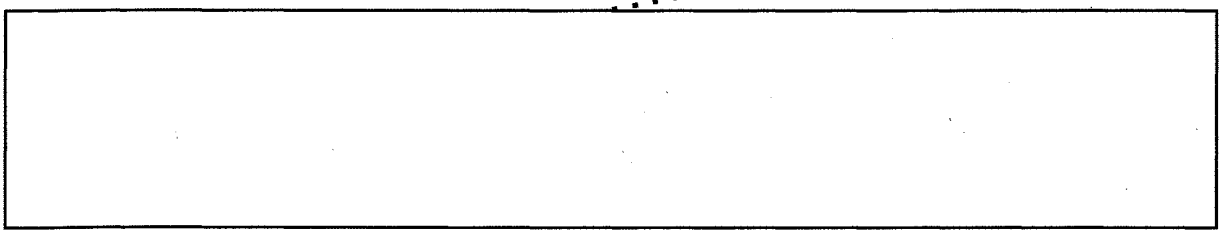
(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



(~~S//SI~~) Tom recalls that the cryptanalysts in his early days, especially, had a real "junk yard dog" mentality: even

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36



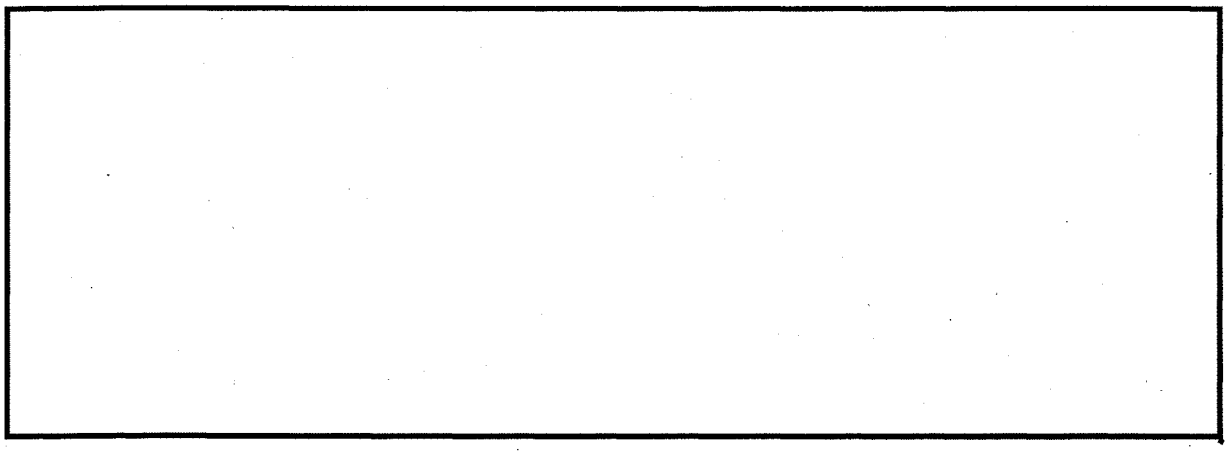
back to top

(b)(3)-P.L. 86-36

(U) GOLDBUG AWARD

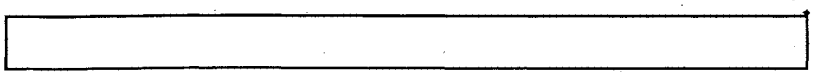
(U//~~FOUO~~) The Cryptanalysis Skill Community takes great pleasure in announcing that the Gold Bug Team Award for excellence of achievement in the field of cryptanalysis has been awarded to [redacted] of IDA-CCS. The recipients were honored in December 2002 at an award ceremony where Ms. Maureen Baginski, Director of SIGINT, gave the congratulatory remarks and presented them with the Gold Bug pins and certificates of achievement. Family members, representatives from the respective organizations, previous award recipients, and other distinguished guests attended the ceremony.

(U) The Gold Bug is an honorary award created by the Cryptanalysis Career Panel in 1982 to recognize outstanding technical excellence and achievement in cryptanalysis by an individual or a team and is approved by the Director NSA. This is the fifth team award that has been given.



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36



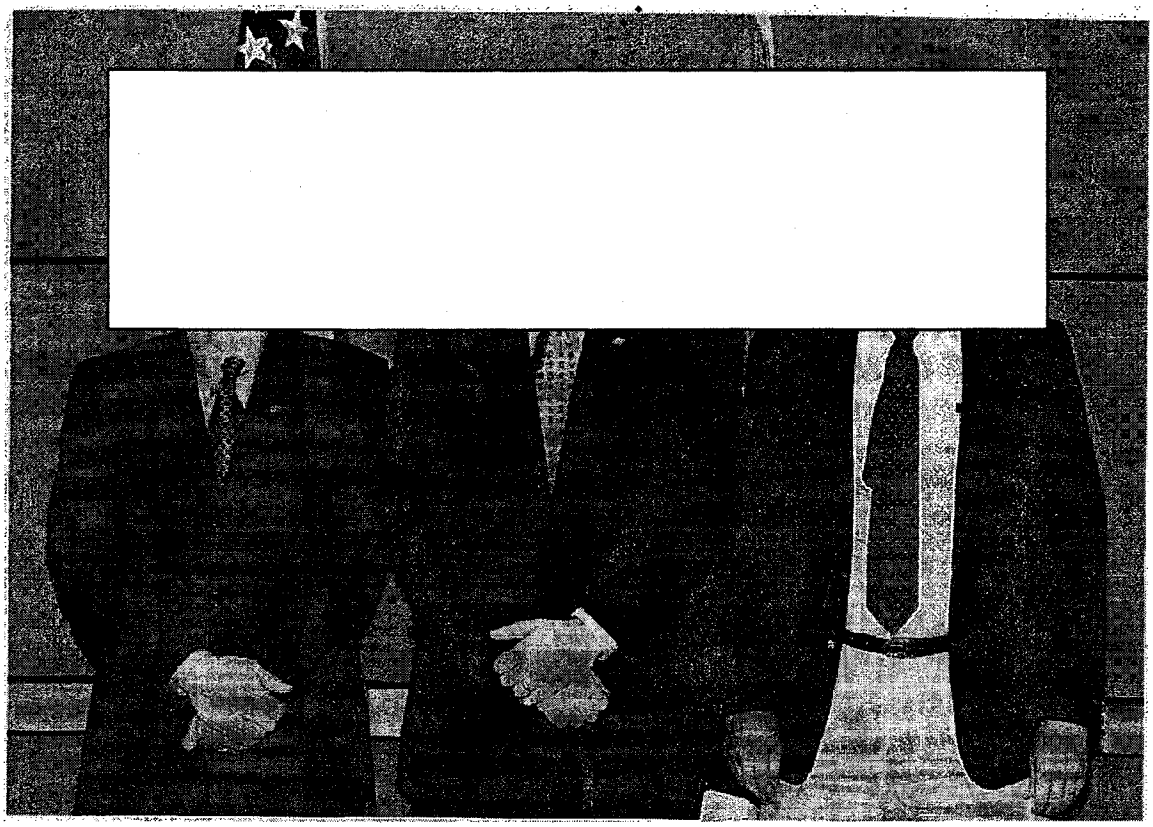


Photo shows from left to right:

back to top

(b)(3)-P.L. 86-36

(U) Meet the Intern -

by

(U//~~FOUO~~) If you get the opportunity to talk about puzzles with you quickly realize that you are not talking to an amateur. He has been a puzzler since the time he could read and has been creating his own since high school (a few of them wound up here, some years before even being employed at the Agency - "Tales of the Krypt", August 1998).

(U) Getting to talk about puzzles is kind of like giving honey to a bear ... no problem, just watch your fingers. He began by explaining to me that the puzzle world is divided into two groups (math and logic puzzles in one group and crosswords in the other), but that his interests reside in both. He personally like to Work math puzzles, but Write crosswords. In addition to Tales of the Krypt (TOTK), He describes a puzzle as being a journey with a destination. Obscurity is a no-no and elegance is a must, especially in crosswords. He says that his puzzles are very much like a movie, with a theme that is well supported. conjectured that the current dilemma in the puzzle world is how computers and automation will affect puzzle generation. He says computers may make the process of creation much easier, but they also take away much of the elegance and human aspect evident in the many of the best puzzles.

(b)(6)

pure research. The work here is more product oriented, and he is better suited for that. Any present frustration that he may have is a result of solving puzzles that are not made to be broken. That can be overlooked, however, by the one characteristic he has found unique to cyptanalysis: when you're done you're done and the work can be put to rest, which makes a puzzler very happy.

(b) (6)

[redacted]

Meet the Intern *is a regular feature of TOTK. Individuals are encouraged to interview Cryptanalysis interns and send contributions to* [redacted] *for publication in this forum. This feature is meant to be informative and light, if not outright funny... never degrading.*

(b)(3)-P.L. 86-36

back to top

DERIVED FROM: NSA/CSS MANUAL 123-2
DATED: 24 FEB 1998
DECLASSIFY ON: X1

~~TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, AND NZL//X1~~

(b)(3)-P.L. 86-36

[redacted]